APLICACIÓN DE LA NORMA NTC 5722 EN LA CONSOLIDACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA UNA ENTIDAD BANCARIA

CRISTINA ALARCÓN TAPIERO

CESAR AUGUSTO HERRERA AGUDELO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2020

APLICACIÓN DE LA NORMA NTC 5722 EN LA CONSOLIDACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA UNA ENTIDAD BANCARIA

CRISTINA ALARCÓN TAPIERO

CESAR AUGUSTO HERRERA AGUDELO

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente: Ing. ALFONSO LUQUE ROMERO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

Nota de aceptación

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Dedicatoria

Dedico este proyecto de grado en primera medida a Dios, quien ha estado presente en las grandes decisiones de mi vida y mis metas trazadas. A nuestro asesor de proyecto el Ing. Alfonso Luque, por su gran apoyo y compromiso para la elaboración de este proyecto. A los Ingenieros Sandra Bernate y Diego Osorio quienes compartieron sus conocimientos y tiempo en desarrollo de esta idea. A mi esposo Wilson Castillo por su paciencia y ánimo. Finalmente, a todos los que estuvieron ahí para así culminar satisfactoriamente este nuevo logro.

Ing. Cristina Alarcón Tapiero.
Especialista en Auditoria de sistemas de Información
Universidad Católica de Colombia

Agradecimientos

Agradezco a Dios por conducirme en mi camino y permitirme concluir con mi objetivo, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer, por haber ubicado en mi horizonte a las personas que han sido auténticos pilares de vida, mi esposo por su apoyo incondicional, por cuidarme y darme fortaleza para continuar en los momentos en los que quería claudicar, por ser la luz de mis días. A mi madre, a mi hermana Gelito y a mi pollo por estar siempre para mí, animándome a superarme constantemente.

Ing. Cristina Alarcón Tapiero.
Especialista en Auditoria de sistemas de Información
Universidad Católica de Colombia

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

1. INTRODUCCIÓN

El concepto de continuidad del negocio empezó a darse a conocer en los años 70, iniciando como un concepto básico de recuperación de desastres, las organizaciones debido al avance tecnológico de la época, empezaron a reconocer la alta dependencia tecnológica en que se estaban adentrando para poder soportar el crecimiento de la industria. Los sistemas computarizados dejaron de ser simples herramientas funcionales para convertirse eventualmente en la base centralizada de su operación. Aunque en aquella época los métodos que podían manejar los computadores eran limitados en comparación, y en su mayoría eran procesos aislados que corrían en grandes computadoras centrales, un daño o bloqueo de una computadora podía durar días, dejando a la compañía expuesta a grandes pérdidas. Entonces se empezó a desarrollar un pequeño sector empresarial que proveía centros de cómputo de respaldo, el costo de este servicio era menor a la posible pérdida que conllevaba detener la operación, o el costo que significaba adquirir más equipos que soportan la operación. Y fue así como a finales de los años 70 esta estrategia se erigió como la opción de recuperación de desastres más utilizada, siendo aún considerado al día de hoy como una importante opción para el respaldo de una operación en caso de siniestro.

Las siguientes dos décadas trajeron consigo una mayor dependencia hacia las computadoras, debido a la aparición de los sistemas abiertos, y el procesamiento de los datos en tiempo real, demostrando que una falla en su sistema tenía impacto directo sobre la continuidad del negocio.

> Pero el concepto continuidad del negocio llegó junto con la aparición del internet desde la década de los noventa e inicios del 2000, consigo organizaciones de todos los tamaños se volvieron mucho más dependientes de la disponibilidad de sus sistemas informáticos. Pero fue con el atentado del 11 de septiembre en Nueva York que las compañías se dieron cuenta del impacto ante un siniestro de esas características en donde además de perder la totalidad de los sistemas informáticos, se perdieron el edificio donde se contenían y más importante aún las vidas de las personas que las operaban. El tener un sistema de continuidad del negocio desarrollado y robusto, les permitiría afrontar esta clase de hechos. El 9/11 contribuye al crecimiento de industrias relacionadas a la recuperación ante desastres, creando desde soluciones de alta disponibilidad hasta infraestructuras de sitios alternos (hot-sites[1]) ,y a la consolidación de la disciplina de continuidad de negocios.[2]

En la actualidad es indispensable para una organización realizar una continua

[1] Hot_site: Normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad. Fuente: https://www.sisteseg.com/sindustrial.html

[2] Business Continuity - Perú, «Antecedentes históricos de la Continuidad del Negocio». (09 07 2012). [En línea]. Available: https:// http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html. [Último acceso: 24 09 2019]

evaluación de sus procesos, buscando el mejoramiento continuo de sus métodos de trabajo, y compararlos con lineamientos internacionales que les permitan frenar cualquier tipo de amenaza.

Este proyecto busca realizar una comparación entre el BCP (Business Continuity Plan) existente, el cual fue elaborado como un desarrollo propio por la entidad bancaria, y alinearlo bajo la norma internacional de continuidad de negocio NTC 5722 la cual nos permite identificar los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.

El interés académico de realizar este proyecto, nos proporciona una base de entendimiento, para el desarrollo e implementación de continuidad del negocio dentro de la entidad bancaria, permitiéndonos identificar los objetivos estratégicos, productos, servicios claves, tolerancia al riesgo, así como el cumplimiento de las obligaciones reglamentarias que hacen referencia a continuidad del negocio.

El contraste del actual BCP contra la norma NTC 5722 nos permitirá generar un análisis GAP por medio del cual se examinen las oportunidades de mejora en el BCP creado y aplicado por la entidad bancaria.

2. GENERALIDADES

2.1. LÍNEA DE INVESTIGACIÓN

La línea de investigación que se adopta en el presente proyecto es: “Software inteligente y convergencia tecnológica”.

2.2. PLANTEAMIENTO DEL PROBLEMA

Las instituciones bancarias tienen como objeto social el manejo del recurso económico de sus clientes y la protección de su dinero para producir flujo de caja y rentabilidad para sí mismo y para sus abonados, ofreciendo productos y servicios encaminados a solventar necesidades de recursos e inversión. Dado lo anterior, son organizaciones que pueden verse afectadas por amenazas que puedan llegar a darse como un riesgo materializado para la organización.

Actualmente, el incremento de las amenazas lógicas, físicas, internas y/o externas han llevado a las entidades bancarias a desarrollar planes y protocolos que permitan una recuperación de sus actividades sin afectar la prestación del servicio hacia sus usuarios y clientes. Este es uno de los motivos por los que un plan de continuidad de negocio es necesario, para asegurar que la operación bancaria proteja de forma integral la información que posee de cada uno de sus clientes, y garantizando la prestación de los servicios hacia sus abonados, guardando en gran medida la integridad de sus datos, enseres, inmuebles y personas que se encuentren adscritos a la organización, lo que ha llevado que en la actualidad, un **BCP** (plan de continuidad del negocio por sus siglas en inglés) sea un factor de obligatorio cumplimiento a lo largo de la prestación y custodia de los servicios bancarios.

Por tanto, se genera una gran preocupación por parte de las empresas del sector bancario y en específico de la entidad bancaria por el estado de madurez con el cual se encuentra constituido su BCP corporativo, por medio del cual tiene las directrices para enfrentar las amenazas y generar la debida protección de sus procesos de negocio y de su actividad social y económica, de cara a la prestación del servicio hacia sus clientes y abonados.

Tomando en consideración lo anteriormente expresado, la entidad bancaria ha realizado un trabajo relacionado con la protección de su negocio el cual fue

elaborado como un desarrollo propio de la entidad basándose en sus particularidades. Sin embargo, dentro de su proceso de mejora continua busca fortalecer sus normas, políticas y procedimientos relacionados con el **BCP** haciendo uso de estándares certificables en el mercado como es el caso de las normas generadas por la Organización Internacional de Normalización (ISO – International Standard Organization) y haciéndolos consistentes con lo descrito en la norma ISO 22301 conocida en Colombia como NTC 5722 la cual recoge los requisitos a tener en cuenta para la implementación del Sistema de Gestión de la Continuidad de Negocio.

2.2.1. Antecedentes del problema

A inicios del siglo XXI se ha agudizado la manifestación de nuevas amenazas e incertidumbres que van desde la llamada guerra contra el terror, el cambio climático y la posibilidad de pandemias que afecten el diario vivir de la humanidad. En poco tiempo, el desarrollo de una nueva crisis ha opacado y superado a otras ya existentes: la crisis financiera que amenaza la economía de muchos países ha empezado por los más desarrollados; sin embargo, sus consecuencias son ya visibles en casi todo el planeta[3].

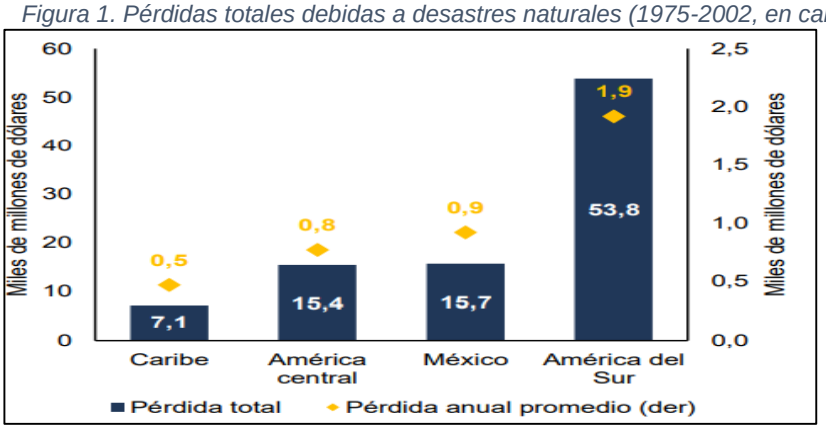
En el caso del sector financiero, los desastres naturales pueden afectar sus actividades de manera directa e indirecta. La primera debido a la interrupción de las operaciones cuando se pierden vidas y se destruyen edificios o equipos; y la segunda a través del impacto recibido por sus diferentes grupos de interés como clientes, proveedores y socios de transacciones. En este sentido, el volumen total del mercado se ve afectado de forma negativa independientemente de si el impacto fue directo o indirecto para la entidad bancaria. Así mismo, las instituciones de crédito, especialmente los bancos, desempeñan un papel importante en el proceso de recuperación económica después de un desastre natural. Cuando los bancos sufren daños físicos o de capital como resultado de una catástrofe, es posible que no se puedan proporcionar los fondos suficientes o a las mismas tasas de interés que antes. Si se opta por el crédito como medida de contingencia para reparar o reemplazar edificaciones o para suplir necesidades básicas afectadas por el desastre natural, se encarecerían los fondos prestables e incluso podrían escasear.

En las últimas décadas se han presentado algunos de los terremotos más devastadores en la historia de la región (Haití 2010, Chile 2010, Ecuador 2016, México 2017). En algunos de estos casos se han decretado estados de excepción y calamidad debido al gran número de afectados y a la magnitud de destrucción de infraestructura, llegando incluso a activar protocolos de ayuda internacional como en el caso haitiano.

[3] DELGADILLO, D., FLORES, I., HERNANDEZ, R., & SANDOVAL, M. «Fondo de información y Documentación para la Industria INFOTEC» «Propuesta de intervención para la continuidad de negocio en trámites y servicios electrónicos del Gobierno Mexicano» (2009). [En línea]. Available: http://infotec.repositorioinstitucional.mx/jspui/handle/1027/234 [Último acceso: 11 10 2019]

De modo que, bajo esta óptica, surge la pregunta de si el sector financiero colombiano está preparado para reaccionar asertivamente ante una eventual emergencia producida por un terremoto. La figura 1 representa la historia de pérdidas económicas como consecuencia de los riesgos naturales en América Latina y el Caribe, que, entre 1975 y 2002, alcanzaron un promedio anual de USD 3.400 millones.

Figura 1. Pérdidas totales debidas a desastres naturales (1975-2002, en cantidades nominales)



Fuente: BID (2012) Elaborado por Asobancaría (2018).

En este sentido, y velando porque el sector tenga la capacidad de responder ante un escenario de crisis, la Superintendencia Financiera de Colombia (SFC) requirió que las entidades financieras extendieran la obligación de tener un plan de continuidad a sus proveedores críticos, lo cual permitiría asegurar que los canales de las entidades tercerizadas tengan un plan de prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

Si bien las entidades y autoridades financieras, al igual que el Gobierno Nacional, han formulado planes para garantizar una respuesta efectiva en la reanudación de las actividades correspondientes de cada uno tras la ocurrencia de un desastre natural, es importante evaluar si existen definiciones claras de cómo se van a integrar estos procesos[4].

Tomando en consideración lo anteriormente expresado, la entidad bancaria ha realizado un trabajo relacionado con la protección de su negocio por cuenta propia. Sin embargo, dentro de su proceso de mejora continua busca fortalecer sus normas, políticas y procedimientos relacionados con el BCP haciendo uso de estándares certificables en el mercado como es el caso de las normas generadas por la Organización Internacional de Normalización (ISO – International Standard Organization) y haciéndolos consistentes con lo descrito en la norma ISO 22301 conocida en Colombia como la norma NTC 5722, la cual recoge los requisitos a seguir por el Sistema de Gestión de la Continuidad de Negocio.

[4] Asobancaría, «¿El sector financiero está preparado ante el riesgo de un desastre natural?». Semana Económica, (24 09 2018) Edición 1155, págs. 2 – 7 [En línea]. Available: https://www.asobancaria.com/wp-content/uploads/1155.pdf. [Último acceso: 11 10 2019]

2.2.2. Pregunta de investigación

¿Cómo se puede fortalecer el BCP de una entidad bancaria adoptando como marco de referencia principal la norma NTC 5722 armonizado con las mejores prácticas de continuidad del negocio?

2.2.3. Variables del problema

- El porcentaje de cumplimiento evaluado con un puntaje definido en el rango de valores contemplado en la medición.
- Recomendaciones de fortalecimiento del BCP según lo enmarcado en la norma NTC 5722.
- La implementación de un modelo de BCP corporativo consistente con los modelos, estándares o recomendaciones de entidades certificadoras de planes de continuidad de negocio.

2.3. JUSTIFICACIÓN

Las entidades financieras son constantemente víctimas de diferentes ataques o eventos que comprometen la ejecución normal de sus labores diarias, repercutiendo directamente sobre sus finanzas, afectando su reputación y la confianza de los clientes e inversionistas, esto sumado a la creciente bancarización en los diferentes estratos económicos aumentando el número de transacciones por año, ha contribuido a que el impacto de estas situaciones sea más grande.

"De acuerdo con la información reportada a la Superintendencia financiera de Colombia (SFC), en el primer semestre de 2019 el sistema financiero colombiano realizó 3.952.962.860 operaciones; 1.665.229.148 monetarias por $3.950 billones y 2.287.733.712 no monetarias"[5]. Por este motivo es de gran importancia que todas las operaciones financieras físicas o lógicas tengan el respaldo suficiente en caso de presentar alguna falla que impida la prestación de su servicio con normalidad, puesto que cada vez son más las operaciones del sistema financiero.

En la tabla se relacionan los canales financieros, con el número de operaciones y el monto total manejado durante el primer semestre de 2019, dilucidando así las posibles afectaciones financieras que tendrían las entidades bancarias, si alguno de

[5] Superintendencia Financiera de Colombia, «Informe de Operaciones Primer semestre 2019» (10 09 2019). [En línea]. Available: https://www.superfinanciera.gov.co/publicacion/61066 [Último acceso: 24 09 2019].

sus servicios prestados en los diferentes canales sufriera un fallo y los dejara inoperantes. Esta es una de las principales razones para contemplar un sistema de continuidad de negocios robusto apoyado en una normativa internacional como las ISO 22301 conocida en Colombia como la norma NTC 5722.

Tabla 1. Resumen general del sistema primer semestre 2019

Canal	Cantidad	Número total de operaciones	Monto de operaciones
Internet	0	851.922.033	1.687.154.490
Oficinas	6.278	267.002.952	1.328.838.979
ACH	0	56.365.735	584.265.432
Cajeros Automáticos	16.080	452.028.751	141.204.299
Corresponsales Bancarios	141.327	185.499.176	68.248.769
Datáfonos	458.631	362.795.179	56.546.121
Débito Automático	0	67.062.301	41.772.924
Telefonía Móvil	0	1.667.229.014	41.270.234
Audio Respuesta	0	43.057.749	917.509
TOTAL		3.952.962.860	3.950.218.761

Fuente: Superintendencia Financiera de Colombia. *[3]*

Existen muchas amenazas y vulnerabilidades por explotar dentro de una entidad bancaria, pero lo que hace fuerte la credibilidad de estas organizaciones es la capacidad que tengan para responder a estos ataques o eventos adversos, como los nombrados a continuación:

Caída o interrupciones en los sistemas de información: Las entidades financieras usualmente cuentan con redundancia en sus sistemas como forma de contención en caso de que alguno de sus componentes presente alguna falla, pero no siempre son lo suficientemente grandes para solventar una crisis como la caída masiva de los servidores o plataformas tecnológicas que soportan sus servicios Bancarios.

El jueves 15 de marzo de 2019 en pleno día de pago, Bancolombia presentó fallas en todos sus canales bancarios a nivel nacional. “El banco indicó que efectivamente se presentaron fallas en varios canales como la Sucursal Virtual Personas, Empresas, aplicación móvil, en las entidades físicas y corresponsales” [dejando sin dinero y posibilidad de transacciones electrónicas a todos sus clientes, adicional a ello, por las numerosas llamadas a sus líneas de atención al cliente colapsaron el sistema de atención, las quejas por las diferentes redes sociales llamaron la atención de la superintendencia financiera, quien ratificó que todos los gastos

asociados a esta pérdidas de servicios debían ser asumidas por la entidad Bancaria”[6].

En la figura 2 “se muestran los reclamos por cuentas de ahorro durante el segundo trimestre de 2019 registrando 66.351 reclamos, la mayoría de quejas en trámite durante el periodo están asociadas a fallas en cajeros automáticos. Estas ascendieron a 30.861, y si bien mermaron, la reducción sólo fue de 1,2% de acuerdo con la Superfinanciera”[7].

Figura 2. Reclamos por cuentas de ahorros lapso enero-marzo/ 2019

Fuente: [https:// www.larepublica.co/finanzas/fallas-en-cajeros-y-descuentos-sin-razon-quejas-de-las-tarjetas-debito-2909557](https://www.larepublica.co/finanzas/fallas-en-cajeros-y-descuentos-sin-razon-quejas-de-las-tarjetas-debito-2909557)

Huelga o paros: El cierre de oficinas por manifestaciones es común en Colombia, las entidades financieras lo hacen con el fin de que sus establecimientos no sean atacados generando destrozos y una posible afectación a mediano o largo plazo.

En Colombia, en el marco de las protestas o también denominadas paro nacional, iniciadas el 21 de noviembre de 2019, la Asobancaría (Asociación Bancaria y de Entidades Financieras de Colombia), advirtió *“Varios establecimientos no prestarían servicio al público, esto debido a que en anteriores ocasiones por donde se*

[6] El Colombiano, «Bancolombia presentó fallas a nivel nacional en pleno día de quincena» (15 03 2018). [En línea]. Available: https://www.elcolombiano.com/antioquia/bancolombia-presenta-fallas-a-nivel-nacional-CJ8391620. [Último acceso: 26 09 2019].

[7] La República, «Fallas en cajeros y descuentos sin razón, entre las principales quejas de las tarjetas débito» (18 09 2019). [En línea]. Available: https://www.larepublica.co/finanzas/fallas-en-cajeros-y-descuentos-sin-razon-quejas-de-las-tarjetas-debito-2909557. [Último acceso: 11 03 2020].

movilizaron las marchas, hubo destrozos a las oficinas bancarias" [8]. Los cierres de estas sucursales afectan directamente a los usuarios que no utilizan los servicios virtuales.

Ataques Informáticos; Con el crecimiento de los sistemas informáticos y la dependencia de ellos, ha venido aumentando exponencialmente los ataques informáticos, en 2017 Colombia sufrió el 0.36% de todas las amenazas que se reportaron en América Latina, Colombia es el sexto país en Latinoamérica con mayor número de Ciberataques,12 Ciberataques de programas maliciosos Malware cada segundo que provienen de piratas de Rusia y Estados Unidos, y según el último balance de la Policía Nacional sobre el cibercrimen en Colombia, en el 2017 los delitos informáticos tuvieron un incremento del 28,3%, respecto al año anterior, y afectaron a 446 empresas del país. Estas son solo algunas estadísticas sobre los ciberataques que según la misma publicación para el año 2017 y los años venideros se pronostica un aumento del 35% [9].

ASOBANCARIA en su publicación Semana Económica 2019, edición 1178 "Riesgo cibernético y el futuro de la estabilidad financiera" hace un breve recuento sobre cómo y cuánto puede afectar el riesgo de ciberseguridad la estabilidad financiera. Allí se cita un estudio generado por el FMI (Fondo Monetario Internacional) en donde muestran como los ataques cibernéticos pueden llegar a comprometer desde el 9% al 62% de los ingresos netos de las entidades financieras [10].

Eventos generados por riesgo operativo: En Instituciones financieras es normal encontrar que el manejo de su información y de sus procesos sea confidencial y solo pueda ser conocido al interior de la organización, por lo tanto, hallar procesos internos creados y basados en las buenas prácticas y la experticia propia de sus funcionarios es normal. El desarrollar procesos de esta forma también conllevan un riesgo en cuanto a la manualidad de las herramientas utilizadas y como todo proceso conlleva a vacíos en su estructura. Por esto se pueden presentar errores al momento de la implementación o simplemente en el desarrollo habitual de sus funciones.

Desastres naturales: Colombia debido a su posición geográfica y sus diferentes sistemas montañosos y costeros, está expuesta a cambios climáticos drásticos, que en ocasiones desatan desastres en las diferentes zonas del país. En los últimos cuarenta años, los desastres naturales le han costado al país cerca de **US$ 7.100 millones** de

[8] RCN Radio, «Bancos podrían suspender atención por paro nacional» (12 11 2019). [En línea]. Available: https://www.rcnradio.com/economia/bancos-podrian-suspender-atencion-por-paro-nacional. [Último acceso: 11 03 2020].

[9] Revista Portafolio, «El secuestro de información desangra a las empresas del país» (29 01 2019). [En línea]. Available: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729. [Último acceso: 26 09 2019]

[10] Asobancaria, «Riesgo cibernético y el futuro de la estabilidad financiera». Semana Economica (26 03 2019). Edición 1178, pág. 4, [En línea]. Available: https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf. [Último acceso: 26 09 2019].

acuerdo con **estimativos del Banco Mundial**, aseguró el **ministro de Hacienda, Alberto Carrasquilla** Añadió que “los riesgos de origen natural son considerados un contingente implícito en Colombia y se incluyen en el Marco Fiscal de Mediano Plazo y el Plan Nacional de Desarrollo. Con cifras a diciembre de 2017 la ocurrencia de desastres se constituye en el contingente más importante para el país (5,2% del PIB), considerando únicamente dos eventos: 1) sísmico y 2) Fenómeno de La Niña**”.**, Entre 1970 y 2011 se han registrado más de 28.000 eventos desastrosos y a partir de la década de 1990 se han presentado alrededor de 60% de estas calamidades naturales. Cualquier evento de esta naturaleza puede afectar directa o indirectamente el sistema bancario colombiano[11].

2.4. OBJETIVOS

2.4.1. Objetivo general

Generar recomendaciones para fortalecer el BCP elaborado por la entidad bancaria mediante un análisis GAP frente a los requerimientos de la norma NTC 5722.

2.4.2. Objetivos específicos

- Comparar las políticas, documentación y procesos recopilados de la por la entidad bancaria, para definir el estado actual del sistema y lo que falta para alcanzar la conformidad con la norma NTC 5722.
- Desarrollar un análisis GAP, contrastando la metodología internacional NTC 5722, para identificar las opciones de fortalecimiento del BCP actual de la entidad bancaria.
- Generar las recomendaciones a partir de los hallazgos que le sirva de referencia a la entidad bancaria para a futuro cumplir con lo establecido en la NTC 5722.

[11] Caracol Radio, «Desastres naturales le han costado al país US$ 7.100 millones» (08 05 2019). [En línea]. Available: https://caracol.com.co/radio/2019/05/08/economia/1557324643_909854.html. [Último acceso: 11 03 2020].

3. MARCOS DE REFERENCIA

3.1. MARCO CONCEPTUAL

Tratar con **Continuidad del negocio** es hablar de la "capacidad de la organización para continuar con la entrega de productos a los niveles predefinidos aceptables después de un evento perjudicial", entendiendo como **evento** la "ocurrencia o cambio de un conjunto particular de circunstancias", estos eventos se pueden materializar como **incidentes** los cuales son una "situación que sería o podría llevar a una interrupción, pérdida, emergencia o crisis", los incidentes pueden materializarse como un **riesgo** siendo este el "efecto de la incertidumbre sobre los objetivos"[12].

Un **sistema de gestión de continuidad de negocio (BCMS**, por sus siglas en inglés) "parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa mantiene y mejora la Continuidad de Negocio" tomando como pilar los procesos de la entidad donde se implementa, entendiendo como **proceso** el "conjunto de actividades interrelacionadas o que interactúan, las cuales transforman entradas en salidas"**,** siendo los procesos el insumo para realizar el **plan de continuidad del negocio** el cual recopila los "procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción", cobrando importancia la **Interrupción máxima aceptable** (**MAO**, por sus siglas en inglés). Siendo este "el tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto / servicio o realizar una actividad, se conviertan en inaceptable"[13].

Dentro del sistema de gestión de continuidad de negocio se establece el **Objetivo mínimo de continuidad de negocio (MBCO**) siendo este el mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción, el **(MBCO**) define el **Punto objetivo de recuperación (RPO)** siendo este el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra y el **Tiempo objetivo de recuperación (RTO)** siendo este el periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra[14].

---

[12] Icontec, «Norma Técnica Colombiana NTC 5722» Sistemas de Gestión de Continuidad de Negocio _ Requisitos, Bogotá, Icontec, 2012, pág. 2-4

[13] Icontec, «Norma Técnica Colombiana NTC 5722» Sistemas de Gestión de Continuidad de Negocio _ Requisitos, Bogotá, Icontec, 2012, pág. 2-5,6

[14] Icontec, «Norma Técnica Colombiana NTC 5722» Sistemas de Gestión de Continuidad de Negocio _ Requisitos, Bogotá, Icontec, 2012, pág. 5,6

3.2. MARCO TEÓRICO

3.2.1. Norma NTC 5722

La norma NTC 5722 “específica los requisitos para la creación y gestión de un Sistema de Gestión de Continuidad de Negocio (BCMS, por sus siglas en inglés) efectivo.

Un BCMS hace énfasis en la importancia de:

- Entender las necesidades de la organización y la necesidad de establecer una gestión de continuidad de negocio, sus objetivos y política.
- implementar y operar los controles y medidas para administrar la capacidad general de una organización en responder a incidentes.
- Hacer el seguimiento y revisión de la eficacia del BCMS
- Mejorar continuamente basado en mediciones objetivas.

El BCMS, como todos los sistemas de gestión, contiene los siguientes componentes claves:

a) Una política

b) Personas con responsabilidades definidas

c) Gestión de los procesos relativos a:

- Política
- Planeación
- Implementación y operación,
- Evaluación de desempeño,
- Análisis de la gestión, y
- Mejoramiento.

d) Documentación que proporcione evidencia auditable; y

e) cualquier proceso de gestión de la continuidad de negocio pertinente para la organización.

La Continuidad de Negocio contribuye a una sociedad con mayor resiliencia. La comunidad en general y el impacto del ambiente organizacional en la organización y en

otras organizaciones, podrían estar involucrados en el proceso de recuperación[15].

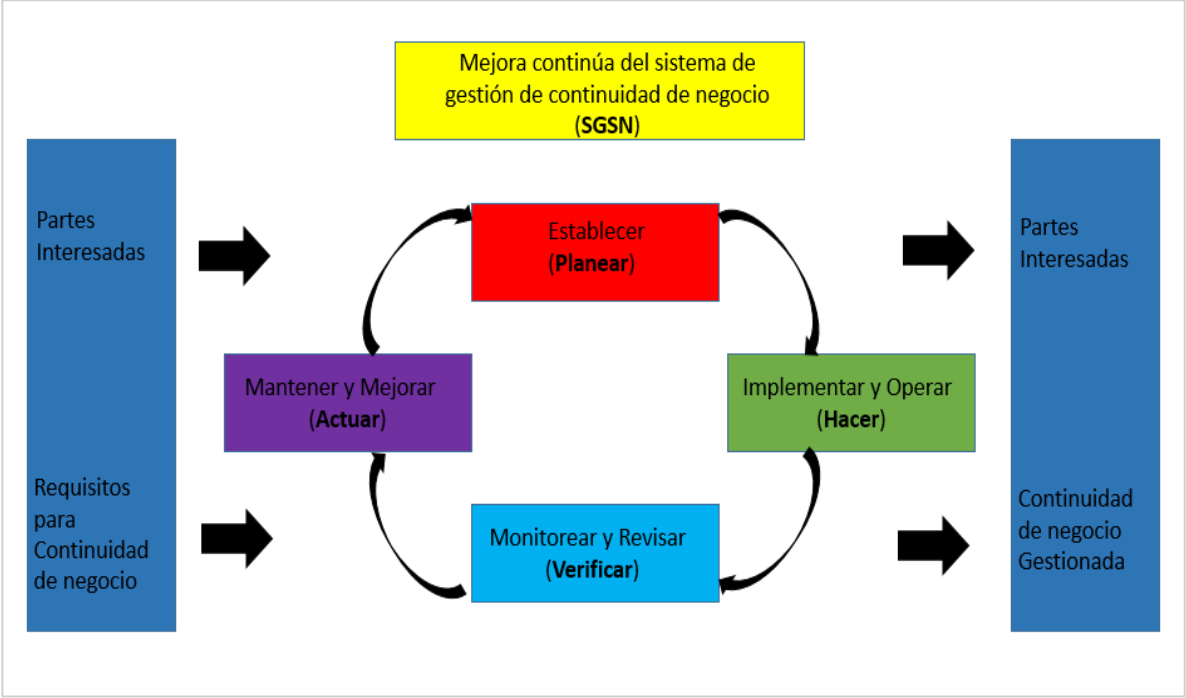
Componentes del PHVA en la norma NTC 5722

La norma **NTC 5722** aplica el modelo "**Planear-Hacer-Verificar-Actuar** (PHVA)" para planear, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la eficacia de un sistema de gestión de Continuidad de negocio en la organización.

Esto asegura un cierto grado de coherencia con otras normas de sistemas de gestión, tales como la norma NTC-ISO 9001 Sistema de Gestión de Calidad, NTC-ISO 14001, Sistema de Gestión Ambiental, NTC-ISO-IEC 27001 Sistema de Gestión en Seguridad de la Información, ISO-1EC20000-1 Gestión de servicios, y la norma NTC ISO 28000 Sistema de gestión de Seguridad para la Cadena de Suministro, de este modo, que la implementación y operación sean consistentes e de gestión relacionados.

La **Figura 3** ilustra cómo un Sistema de Gestión de continuidad de Negocio (**BCMS**) toma como entradas las partes interesadas y los requisitos para la gestión de la continuidad y atreves de las acciones y procesos necesarios, produce resultados de la Continuidad de negocio (gestión de continuidad de negocio) que cumplen con esos requisitos.

Figura 3. Ciclo PHVA aplicado a los procesos de BCMS



[15] Icontec, «Norma Técnica Colombiana NTC 5722» de Sistemas de Gestión de Continuidad de Negocio _ Requisitos, Bogotá, Icontec, 2012, pág. I

Fuente: NTC 5722 pág. II

Tabla 2. Explicación del modelo de PHVA

Ciclo	Descripción
Planear (Establecer)	Establecer política, objetivos, metas, controles, procesos y procedimientos de continuidad de negocio pertinentes para mejorar la continuidad de Negocio, con el fin, de entregar resultados que se alineen con todos los objetivos y políticas de la organización.
Hacer (Implementar y Operar)	Implementar y operar la política, controles, procesos y procedimientos de Continuidad de Negocio.
Verificar (Monitorear y revisar)	Monitorear y revisar el desempeño contra la política y los objetivos de continuidad de negocio, reportar los resultados a la Dirección para la revisión, y determinar v autorizar las acciones para la reparación y mejoramiento.
Actuar (Mantener y mejorar)	Mantener y mejorar el BCMS tomando acción correctiva, basada en los resultados de la revisión por la Dirección y la revalorización del objeto del BCMS y la política y los objetivos de continuidad de negocio.

Fuente NTC 5722 pág. III

En el modelo PHVA como se muestra en la Tabla 12, desde el Contexto de la organización al ítem de mejora de esta norma, se cubren los siguientes componentes:

- El Contexto de la organización en el numeral 4 es un componente del Planear. Introduce los requisitos necesarios para establecer el contexto del BCMS que se aplica a la organización, así como las necesidades, requisitos y alcance.
- El Liderazgo en el numeral 5 es un componente del Planear. En él se resumen los requisitos específicos del papel de la alta dirección en el BCMS y cómo el liderazgo articula sus expectativas a la organización por medio de la declaración de la política.
- La Planificación en el numeral 6 es un componente del Planear. En él se describen los requisitos de lo que se refiere al establecimiento de objetivos estratégicos y los principios que rigen el BCMS en su conjunto. El contenido de este ítem difiere del establecimiento del plan del tratamiento del riesgo como consecuencia de la valoración del riesgo de continuidad, así como el análisis de impacto en el negocio (BIA) de los cuales generan los objetivos de recuperación del negocio.
- Los recursos en el numeral 7 son un componente del Planear. Es soporte a las operaciones del BCMS lo que se refiere a la determinación de la competencia y la comunicación de forma periódica o según sea necesario, con las partes interesadas, al mismo tiempo documentar, controlar, mantener y conservar la documentación requerida.
- La operación en el numeral 8 es un componente del hacer. En él se definen los requisitos de continuidad de Negocio, determina la forma de abordarlos y desarrolla los procedimientos para administrar un incidente perjudicial.
- La Evaluación de desempeño en el numeral 9 es un componente del Verificar. En él se resumen los requisitos necesarios para medir el rendimiento de la continuidad de Negocio, el cumplimento del BCMS con la norma y sus expectativas de gestión y busca una retroalimentación del sistema respecto a las expectativas.

- La mejora en el numeral 10 es un componente del Actuar. Se identifica y actúa sobre las no conformidades del BCMS a través de una acción correctiva[16].

3.3. MARCO JURÍDICO

En Colombia se han desarrollado por parte del estado leyes, circulares y decretos que hacen referencia al manejo y protección de la información, así como de los respectivos planes de contingencia para la protección de activos, de las cuales se mencionan las que afectan este proyecto:

> **Circular externa No. 004 DE 1999 de la Superintendencia Financiera de Colombia,** Por medio de la cual se dictan las disposiciones para el Plan de pruebas, mitigación del impacto, plan de contingencias y certificación de cumplimiento del año 2000.) deben incluir como parte de su plan de trabajo pruebas sobre todos sus sistemas susceptibles de verse afectados por el problema del año 2000, deben elaborar o ajustar sus planes de contingencia a los posibles siniestros que pueda ocasionar el cambio de milenio y deben documentar todas las actividades desarrolladas a lo largo del proyecto[17].

Teniendo en cuenta que el BCP está basado en establecer las buenas prácticas que debe desarrollar una empresa para sostener su operación dando cumplimiento a la legislación nacional o internacional que proceda según la naturaleza del negocio, la circular externa 004 DE 1999 define las disposiciones sobre las cuales establece que se deben desarrollar pruebas sobre todos sus sistemas.

> En desarrollo de sus operaciones, las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) se exponen al Riesgo Operativo (RO). Por tal razón, dichas entidades deben desarrollar, establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO), acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente este riesgo[18]. Su origen normativo, se encuentra en la **Ley 964 de 2005** del **Congreso de la República de Colombia**, en donde se dictan todas las reglas relativas a la administración de riesgos operativos junto con la **Resolución 1865 de 2007**, las entidades deben: revelar de forma adecuada los gastos y los ingresos de riesgo operativo, para registrar la línea y el tipo de evento en cuentas auxiliares a nivel interno creadas especialmente para ello[19].

---

[16] Icontec, «Norma Técnica Colombiana NTC 5722» de Sistemas de Gestión de Continuidad de Negocio _ Requisitos, Bogotá, Icontec, 2012, págs. II, III.

[17] Superintendencia Financiera de Colombia, «Circular Externa 004 de 1999» (19 03 1999). [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/553/dPrint/1/c/00. [Último acceso: 05 10 2019].

[18] Superintendencia Financiera de Colombia, «Reglas relativas a la administración del riesgo operativo» (06 2007). [En línea]. Available: https://fasecolda.com/cms/wp-content/uploads/2019/08/ce041-2007-anexo.pdf. [Último acceso: 20 04 2020].

[19] ISOTools, «Sistema de Administración del Riesgo Operativo (SARO): ¿Cómo administrar los riesgos?» (18 08 2017). [En línea]. Available: https://www.isotools.com.co/sistema-administracion-del-riesgo-operativo-saro-administrar-los-riesgos/. . [Último acceso: 20 04 2020].

Y **Circular Externa 041 de 2007 de la Superintendencia Financiera** “la cual Modifica el Capítulo XXIII de la Circular Externa 100 de 1995, denominado Reglas Relativas a la Administración del Riesgo Operativo”[20].

Ley 1266 DE 2008 Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones[21].

La ley de Habeas data es importante para el desarrollo del trabajo puesto que se debe dar a los clientes la plena disponibilidad de su información cuando ellos lo requieran así, y no someterlos a la ausencia de esta por fallas en el sistema.

Esta ley junto con **Ley 1273 de 2009 sobre Protección de la información y de los datos**; al Documento Conpes 3701 emitido por el Departamento Nacional de Planeación y establece lineamientos de política para Ciberseguridad y Ciberdefensa. "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[22]. Y la

Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”[23] Este conjunto de leyes ratifica la necesidad de los clientes de contar la plena seguridad y disponibilidad de su información, competiéndole directamente al BCP.

El sistema de control interno dentro de una entidad bancaria recobra gran importancia ya que al ser el conjunto de políticas, principios, procedimientos y mecanismos de verificación y evaluación que establece un grado de seguridad razonable en sus procesos, realizando una adecuada gestión de riesgos, con el fin de formalizar este SCI se genera la **Circular Externa 038 de 2009 de la Superintendencia Financiera de Colombia**, la cual determina las instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI) de las entidades supervisadas[24].Y la

Circular Externa 052 de 2007 Superintendencia Financiera de Colombia en el que

---

[20] Superintendencia Financiera de Colombia, «Circular Externa 041 de 2007» (29 06 2007). [En línea]. Available: https://www.superfinanciera.gov.co/publicacion/20068. [Último acceso: 11 10 2019].

[21] Congreso De La República de Colombia, «Ley estatutaria 1266 de 2008» (31 12 2008). [En línea]. Available: http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf. [Último acceso: 11 10 2019].

[22] Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), «Ley 1273 de 2009» (05 01 2009). [En línea]. Available: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009. [Último acceso: 05 10 2019].

[23] Congreso de la República de Colombia, «Ley estatutaria 1581 de 2012» (18 10 2012). [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 11 10 2019].

[24] Superintendencia Financiera de Colombia, «circular externa 038 de 2009» (29 09 2009). [En línea]. Available: https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile22457&downloadname=ce038_09.doc. [Último acceso: 05 10 2019]

se define que las entidades vigiladas en función de sus operaciones están expuestas a distintos tipos de riesgo. Por este motivo, dichas entidades deben desarrollar, establecer, implementar y mantener planes de continuidad del negocio, definidos como el conjunto detallado de acciones que describen los procedimientos, sistemas y recursos necesarios para retornar y continuar la operación, en caso de interrupción[25] .

Para el fortalecimiento de la estructura de seguridad adherimos la **Circular 022 de julio 30 de 2010 de la Superintendencia Financiera de Colombia** "la cual establece los aspectos relacionados con los requerimientos de seguridad y calidad para la realización de operaciones"[26] y la.
Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia la cual incorpora modificaciones en su capítulo décimo segundo del título de la circular en la cual establece los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales e instrumentos para la realización de operaciones[27].

Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia "La cual establece que las entidades deberán incluir en el plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de un ataque cibernético"[28] Y
Circular Externa 008 de 2010 de la Superintendencia Financiera de Colombia mediante la cual se establecen mecanismos de protección de la información de los consumidores financieros al realizar operaciones monetarias usando los servicios de las pasarelas de pago. En la norma se establecen los estándares de seguridad para que estas plataformas puedan prestar sus servicios a través de las entidades vigiladas por la Superfinanciera (bancos y redes de pago)"[29].

En cuanto a directrices entregadas por el gobierno nacional para la atención de desastres y la estrategia de seguridad informática tomamos como marco para el proyecto

Ley 1523 DE 2012 Política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones, Se constituye en una política de desarrollo indispensable para asegurar la sostenibilidad,

---

[25] Asobancaría, «¿El sector financiero está preparado ante el riesgo de un desastre natural?» Semana económica, (24 09 2018) Edición 1155, pág. 6 [En línea]. Available: https://www.asobancaria.com/wp-content/uploads/1155.pdf. [Último acceso: 03 24 2020].
[26] Superintendencia Financiera de Colombia, «Circular Externa 008 de 2010» (29 03 2010). [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20148/dPrint/1/c/20149. [Último acceso: 05 10 2019].
[27] Superintendencia Financiera de Colombia, «Circular Externa 042 de 2012» (04 10 2012). [En línea]. Available: https://www.superfinanciera.gov.co/publicacion/20142. [Último acceso: 10 09 2019].
[28] Superintendencia Financiera de Colombia, «Circular Externa 007 de 2018» (05 06 2018). [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00. [Último acceso: 03 24 2020]
[29] Superintendencia Financiera de Colombia, «Circular Externa 008 de 2018» (05 06 2018). [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00. [Último acceso: 03 24 2020]

la seguridad territorial, los derechos e intereses colectivos[30]. Y él **Decreto 2573 de 12 de diciembre de 2014** "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones"[31].

3.4. ESTADO DEL ARTE

Se puede evidenciar en estudios desarrollados a nivel internacional diferentes aportes, como el planteado por Jairo Rojas en el año 2017 para la **Universidad De Las Américas Ecuador** en su proyecto de grado denominado **Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del ecuador**

, cuyo objetivo General era "Proponer un plan de continuidad del negocio para una institución financiera del sector privado bancario del ecuador" **en donde evidencian las siguientes conclusiones** describiendo su importancia para el desarrollo del presente trabajo**:**

- El autor indica que las amenazas y los riesgos, fueron identificados satisfactoriamente durante el proyecto, asegurando la prevención de los daños, así como las posibles pérdidas que pueden traer consigo la ocurrencia de desastres en el banco y haciendo posible un manejo más eficiente de los recursos.

Lo anterior es un aspecto importante a tener en cuenta en la comparación a realizar entre la norma NTC 5722 y el manual de sistema de gestión de continuidad de negocio de la entidad bancaria, ya que se busca con el cumplimiento de la norma proteger los recursos del banco y conocer los riesgos y vulnerabilidades a los que puede estar expuesto.

- Para establecer la metodología el autor tuvo en cuenta estándares internacionales consistentes con la elaboración de un Plan de Continuidad del Negocio, como por ejemplo lo estipulado en las normas ISO [32].

Guarda relación con nuestro proyecto en la medida que se realiza con el análisis GAP un contraste entre el manual de sistema de gestión de continuidad de negocio de la entidad bancaria y la Norma Técnica Colombiana NTC 5722.

---

[30] Congreso De La República de Colombia, «Ley estatutaria 1581 de 2012» (18 10 2012). [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 11 03 2020].

[31] MinTIC, «Decreto número 2573 de 2014» (12 12 2014). [En línea]. Available: https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf. [Último acceso: 05 10 2019].

[32] ROJAS, J. «Facultad de postgrados UDLA» «Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del ecuador» (2017). [En línea]. Available: http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf. [Último acceso: 11 10 2019]

A nivel nacional se encuentran estudios desarrollados sobre el BCP, el desarrollado por Jhon Torres y Heiner Velazco en el año 2014 para la **Universidad Católica de Colombia** en su proyecto denominado "**Diseño Y Propuesta De Implementación De Un Plan De Continuidad Del Negocio Aplicable A Los Hospitales En La Ciudad De Bogotá,** cuyo objetivo General era "Diseñar y proponer la implementación de un Plan de Continuidad del Negocio que sea aplicable a los Hospitales en la ciudad de Bogotá"**, en donde evidencian las siguientes Conclusiones:**

- Los autores indican que la causa más común para la falta de implementación de un plan de continuidad del negocio, es la falta de recursos monetarios que apoyen este tipo de actividades, además del desconocimiento del tema.
- Sugieren realizar el proceso de una estrategia de continuidad del negocio en los hospitales de Bogotá, que permita proteger las actividades claves de la cadena de valor, la cual debe ser prioritaria y en corto plazo. Esto teniendo en cuenta que existen riesgos naturales tales como terremotos e inundaciones; de hecho, actualmente la ciudad de Bogotá está clasificada como amenaza intermedia de sufrir sismos que podrían llegar a los 7 grados en la escala de Richter.
- Los tres (3) hospitales tienen identificado como parte esencial para su funcionamiento la infraestructura tecnológica, información en medios digitales y el software especializado, sin embargo, no tienen implementados planes ni estrategias que respalden los activos antes señalados [33].

Si bien es cierto que el sector bancario tiene una misión y objetivos distintos al sector bancario en ambas se puede evidenciar el concepto de misión crítica para la operación, presentando aspectos de estudio a considerar en la realización del contraste entre el manual de sistema de gestión de continuidad de negocio de la entidad bancaria y la Norma Técnica Colombiana NTC 5722.

4. METODOLOGÍA

4.1. FASES DEL TRABAJO DE GRADO

Para el desarrollo del proyecto, se realizarán cuatro fases, con el fin de dar cumplimiento a los objetivos:

[33] TORRES, J. y VELASCO, H. «Repositorio universidad católica de Colombia» «Diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de bogotá» (18 11 2014). [En línea]. Available: https://repository.ucatolica.edu.co/bitstream/10983/1706/1/Trabajo%20de%20Investigacion%20BCP%20Hospitales%20de%20la%20Ciudad%20de%20Bogota.pdf. [Último acceso: 02 10 2019]

Fase 1: En ésta primera fase se realizará el análisis del contexto interno de la organización, para lo cual se realizará un levantamiento de información, revisión documental y revisión de políticas para así definir las necesidades de la organización.

Fase 2: En la segunda fase se realizará un análisis GAP por medio del cual se hará un estudio de la distancia entre las prácticas actuales de la organización y aquellas requeridas por la norma NTC 5722, para lo cual se revisará el BCP corporativo y posteriormente se ejecutará un contraste de los procesos de la norma NTC 5722.

Fase 3*:* En esa fase se generará las recomendaciones las cuales serán encaminadas a crear un plan de fortalecimiento a partir de los hallazgos encontrados en las fases anteriores y se generarán las respectivas conclusiones.

Fase 4*:* En esta fase se realizará la entrega del proyecto a la universidad, se realizarán las correcciones al documento si hay lugar a ellas y se hará la respectiva presentación del proyecto.

Figura 4. Fases del trabajo de grado

Fuente: Elaboración de los autores.

4.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Se utilizarán los siguientes Instrumentos o Herramientas en el presente proyecto:

- BCP corporativo de la entidad bancaria.
- Norma ISO 22301 conocida en Colombia como NTC 5722.
- Manuales de procesos (a los que se tengan acceso).
- Políticas (a los que se tengan acceso).
- Herramientas ofimáticas.

4.3. ALCANCE Y LIMITACIONES

4.3.1. Alcance

El fortalecimiento del BCP estará basado en las recomendaciones que se espera que la entidad bancaria implemente frente al análisis de los controles que se encuentran en funcionamiento para garantizar la disponibilidad de la información, el cual se desarrolla con relación a la norma NTC 5722.

El trabajo contempla la revisión y análisis del BCP general corporativo de la entidad bancaria, sin entrar a la identificación individual por área o por proceso de la organización. Utilizando como referente la norma internacional NTC 5722.

El proyecto no pretende únicamente dar las recomendaciones para el BCP corporativo, si no que sirva de elemento de consulta para diferentes entidades que tengan implementado el BCP y pretendan acogerse a los principios que dicta la norma NTC 5722.

4.3.2. Limitaciones

El desarrollo del proyecto no plantea realizar el análisis de los controles individuales por área o proceso de la entidad bancaria.

El análisis no busca identificar la madurez de los controles actuales implementados por la entidad bancaria, busca directamente tomar estos controles y contrastarlos contra la norma NTC 5722, identificando que se utiliza y que no, para crear las recomendaciones de fortalecimiento que brinda la norma.

Se realizará la entrega de un documento con las recomendaciones creadas de acuerdo al análisis y estudio del BCP y la NTC 5722, pero no se implementarán ni se harán las acciones de fortalecimiento.

La información base, es la entregada por la entidad bancaria, a la fecha de inicio del proyecto, y las proyecciones del proyecto están en base a la misma, cualquier cambio, modificaría los entregables y el alcance del análisis.

5. DESARROLLO DE LA PROPUESTA

La ejecución de la propuesta se basa en las fases en 4 fases, definiéndose de la siguiente forma:

5.1. FASE 1: ANÁLISIS DE LA ENTIDAD

La entidad escogida para la evaluación del BCP, es una de las empresas más grandes del país, con más de 800 oficinas cubriendo la totalidad del territorio nacional. Adicionalmente dispone de un completo portafolio de servicios y de un dinámico portal electrónico operando las 24 horas del día. Su capital humano es de más de 12 mil funcionarios, distribuidos en 8 vicepresidencias divididas en actividades operativas, comerciales, financieras y de apoyo (Contraloría, tecnología, estrategia y planeación).

5.1.1. Historia

La entidad bancaria goza de gran trayectoria y reconocimiento a nivel nacional, siendo uno de los bancos más antiguos del país.

5.1.2. Contexto interno

La gerencia de continuidad depende de la vicepresidencia de operaciones de la entidad bancaria, y está compuesta por cinco funcionarios, divididos en dos funcionarios encargados de la elaboración y pruebas de continuidad, dos funcionarios encargados de la sensibilización y capacitación de los planes de continuidad de negocio, y el coordinador del área.

La entidad desarrolló su plan de gestión de continuidad de negocio en el año 2013, y en los años venideros fue sometido a varias actualizaciones y ajustes de su contenido según la actualización de las políticas y estructura organizacional de la entidad bancaria, como lo fue la actualización del BIA en 2016, o la actualización de la evaluación de riesgos de continuidad, por la actualización de proveedores críticos.

Tabla 3. Misión y visión de la entidad bancaria

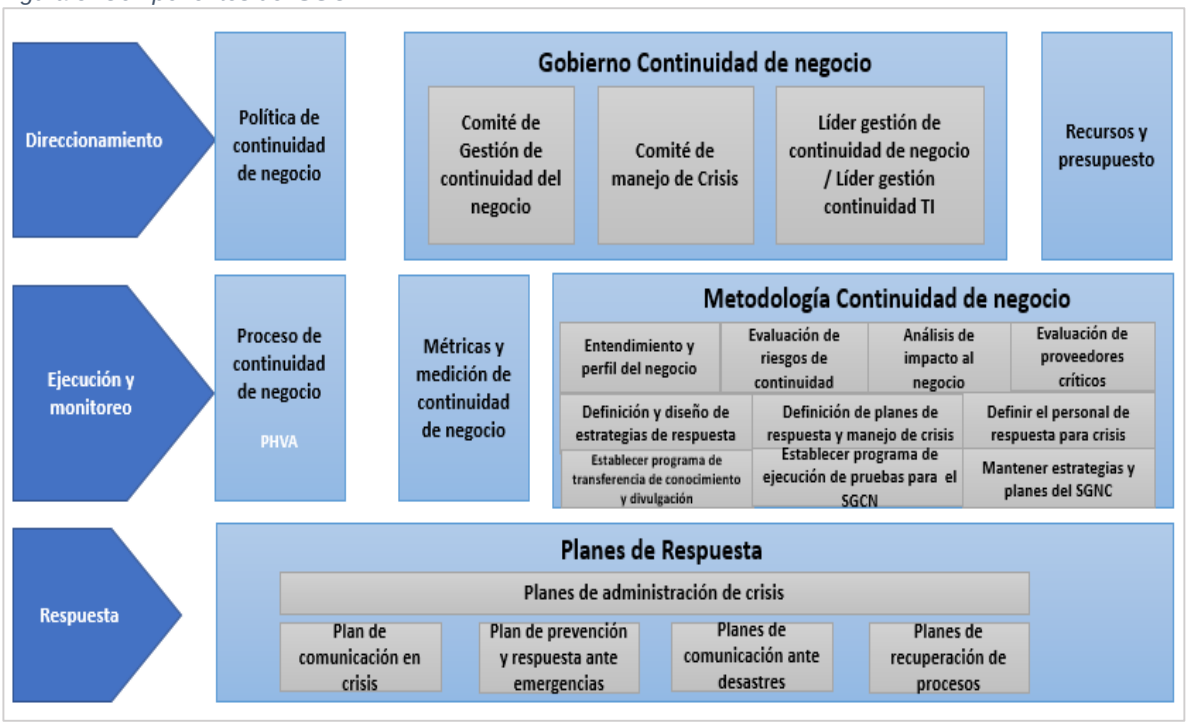
MISIÓN	Acompañar ética y profesionalmente a nuestros clientes en el logro de sus objetivos con bienes y servicios financieros adecuados, generando valor a nuestros colaboradores, accionistas y sociedad en general.
VISIÓN	Ser la entidad bancaria líder y referente en Colombia y Centroamérica, que crece con el progreso de sus clientes, de su equipo humano, de sus accionistas y del país.

Fuente: Elaboración de los autores.

5.1.3. Componentes del sistema de gestión de continuidad de negocio

Se identificaron los siguientes componentes para el sistema de gestión de continuidad del negocio:

Figura 5. Componentes del SGCN

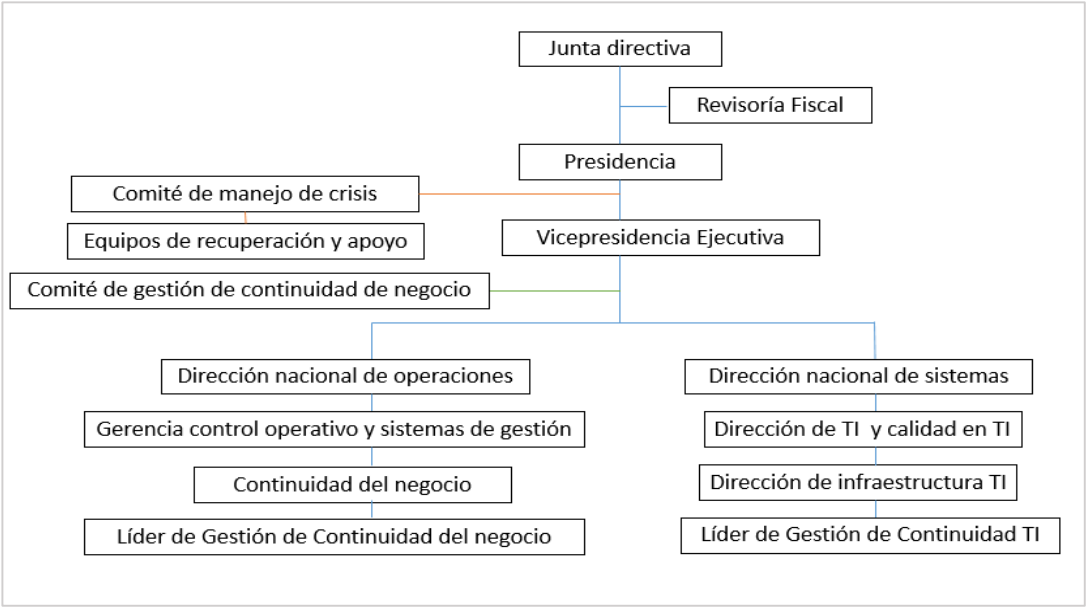


Fuente: Elaboración de los autores.

5.1.4. Organigrama gobierno de continuidad

Dentro del manual de continuidad de negocio generado por la entidad bancaria, se establece el organigrama del gobierno de continuidad de negocio, en el que se aclaran las relaciones, la interacción y el trabajo en equipo de los responsables para asegurar una preparación efectiva ante situaciones de riesgo, desastre o interrupción. Entregando a cada participante de la estructura los roles, niveles de reporte y las responsabilidades de forma tal que se pueda dar sostenibilidad, soporte y mantenimiento continúo al estado de preparación de la organización.

Figura 6. Organigrama Gobierno de continuidad

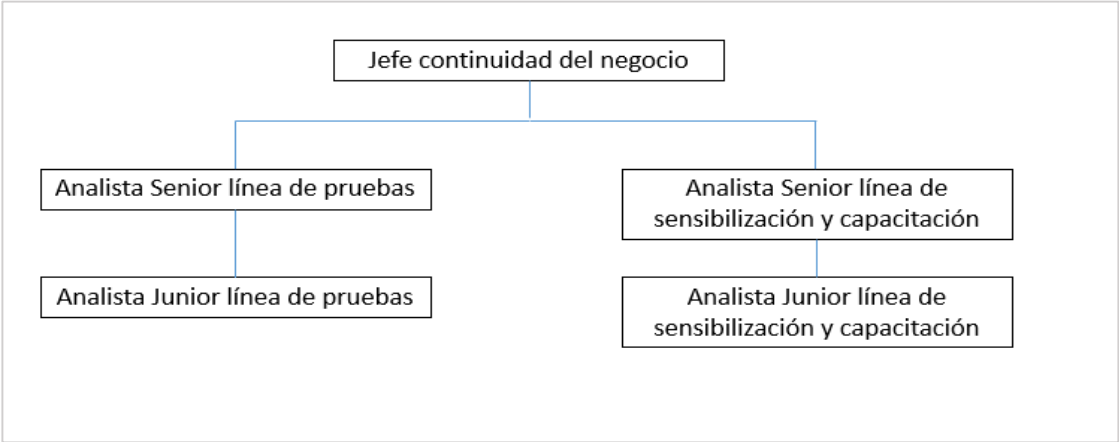


Fuente: Elaboración de los autores.

5.1.5. Organigrama área de continuidad del negocio

El área de continuidad de negocio, es la responsable de regularizar la definición, actualización, implementación y pruebas del SGCN. Debe cerciorarse del empleo, divulgación y entendimiento de la estructura metodológica, política, roles, responsabilidades y definiciones del personal involucrado dentro del sistema.

Figura 7. Organigrama área de continuidad del negocio



Fuente: Elaboración de los autores.

5.2. FASE 2: ANÁLISIS DE INFORMACIÓN DE LA ENTIDAD

5.2.1. Revisión del BCP Corporativo

Se realiza la revisión del BCP corporativo en base al manual “Sistema de gestión de Continuidad del Negocio”, el cual está compuesto de la siguiente manera:

Tabla 4. Secciones del manual del Sistema de gestión de Continuidad del Negocio

Sección	Nombre	Descripción
1	Objetivos	Define el objetivo principal y objetivos secundarios del Sistema de Gestión de Continuidad del Negocio (SGCN) de la entidad bancaria
2	Alcance	Define el alcance del SGCN.
3.1	Principios y lineamientos	Define las normas que rigen el SGNC.
3.2	Gobierno de Continuidad de Negocio	Establece las líneas de administración y trabajo en equipo requerido para asegurar una preparación efectiva ante situaciones de riesgo, desastre o interrupción y define los roles y responsabilidades del personal involucrado en el SGCN.
3.3	Recursos y presupuesto	Define los recursos humanos y económicos para el mantenimiento del SGCN.
3.4	Proceso de gestión continuidad del negocio	Define los lineamientos para establecer, implementar, ejecutar, supervisar, ejercer, mantener y mejorar la efectividad del SGCN .
3.5	Métricas y medición de la gestión de continuidad del negocio	Define los indicadores de gestión del SGNC incluyendo el nivel de cultura de continuidad de los empleados.
3.6	Metodología de Continuidad del Negocio	Define el entendimiento y perfil del negocio, la evaluación de riesgos, el análisis de impacto al negocio y la evaluación de proveedores críticos.

Fuente: Elaboración de los autores.

El manual esta articulado con los siguientes planes de respuesta:

Tabla 5. Documentos complementarios al manual

Tipos de Planes de Respuesta	Descripción
Plan de administración de crisis	Establece los procedimientos que permiten la activación y escalamiento de una crisis o incidente que afecte o pueda afectar la reputación, imagen, u operación de la entidad bancaria.
Plan de comunicación de crisis	Define los lineamientos y procedimientos que utiliza la entidad bancaria para comunicar interna y/o externamente incidentes o eventos que puedan generar una crisis y que afecta directamente a la entidad bancaria; garantizando la claridad y oportunidad en la entrega de información suficiente a través de los medios adecuados.
Plan de prevención, preparación y respuesta ante emergencias	Establece los procedimientos para minimizar las lesiones y pérdidas de vidas humanas, utilizando la estructura y recursos necesarios.
Plan de Contingencia y recuperación de Tecnología – DRP	Establece los procedimientos que permiten mantener la continuidad de la plataforma tecnológica soporte a los procesos críticos de la entidad bancaria, en caso de la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente
Plan de recuperación de procesos	Define los procedimientos que permiten mantener la continuidad de los procesos prioritarios en caso de la ocurrencia de un evento de desastre o interrupción.
Planes o procedimientos de Contingencia de procesos	Define el conjunto de acciones y recursos para responder a fallas e interrupciones internas y externas que puedan afectar la operación normal de un proceso.

Fuente: manual "Sistema de gestión de Continuidad del Negocio", pág. 29.

5.2.2. Contraste de procesos bajo la norma NTC 5722

Dando cumplimiento a la comparación de políticas, documentación y procesos recopilados de la entidad bancaria evidenciables en el manual del SGCN se realiza el contraste de los procesos según el modelo PHVA, desde el numeral 4 al numeral 10 según la norma NTC 5722 la cual cubre los siguientes componentes:

Tabla 6. Contraste de procesos según el modelo PHVA bajo la norma NTC 5722

ISO 22301 / NTC 5722				
PLANEAR	4	CONTEXTO DE LA ORGANIZACIÓN		
	Aparte	**Sección**	**Descripción**	
	4.1	Descripción de la organización y su contexto.	La organización debe identificar y documentar:	Los procesos de la organización, funciones, servicios, productos, asociaciones, cadenas de suministro, las relaciones con las partes interesadas, y el impacto potencial relacionado con un incidente perjudicial.
				Las relaciones entre la política de continuidad de Negocio y objetivos de la organización y de otras políticas, como su estrategia de gestión de riesgo global.
				Apetito de riesgo de la organización.
			Al establecer el contexto, la organización debe:	Articular sus objetivos, incluidos los relativos a la Continuidad de Negocio.
				Definir los factores externos e internos que generan la incertidumbre que da lugar al riesgo.
				Establecer criterios de riesgo, teniendo en cuenta el apetito de riesgo.
				Definir el propósito del BCMS.
	4.2	Entendiendo las necesidades y expectativas de las partes interesadas.		Generalidades
	4.2.1	Generalidades	Cuando se establece un BCM la organización debe determinar:	Las partes interesadas que son pertinentes del BCMS.
				Los requisitos de estas partes interesadas
	4.2.2	Requisitos legales y reglamentarios		
	4.3	Determinar el alcance del sistema de gestión.		
	4.3.1	Generalidades	Se debe determinar el alcance del sistema de gestión.	

PLANEAR	4.3.2	Alcance del BCMS	La organización debe:	Establecer las partes de la organización para ser incluidas en el BCMS.
				Establecer los requisitos de BCMS, teniendo en cuenta la misión de la organización, los objetivos, las obligaciones internas y externas, y las responsabilidades legales y regulatorias.
				identificar los productos, servicios y todas las actividades relacionadas con el alcance del BCMS.
				Tener en cuenta las necesidades de las partes interesadas y los intereses.
				Definir el alcance del BCMS en términos de y apropiado para el tamaño, la naturaleza y complejidad de la organización.
	5	**LIDERAZGO**		
	5.1	Generalidades.	Las personas de la alta dirección y otros roles directivos pertinentes de la organización deben demostrar liderazgo con respecto al BCMS.	
	5.2	Compromiso de la alta dirección.	La alta dirección debe demostrar su liderazgo y compromiso:	
			- Políticas y objetivos.	
			- Integración .	
			- Recursos.	
			- Comunicación.	
			- Resultados.	
			- Mejora continua.	
			La alta dirección asegurar responsabilidades y autoridad.	
			- Definición de criterios de riesgo.	
			- Participando en pruebas.	
			- Asegurar auditorías.	
			- Mejora continua.	
	5.3	Política.	La alta dirección debe establecer y comunicar una política de continuidad de negocio	Ser adecuada para el propósito de la organización.
				Proporcionar el marco para establecer objetivos de Continuidad de Negocio.
				Incluir un compromiso para satisfacer los requisitos aplicables.
				Incluir un compromiso de mejora continua del BCMS.

PLANEAR	5.4	Roles, responsabilidades y autoridades.	La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones pertinentes se asignen y sean comunicadas.	Asegurar que el sistema de gestión se establezca en conformidad con los requisitos de la norma.
				Informar sobre el desempeño del BCMS a la alta dirección.
	6	**PLANIFICACIÓN**		
	6.1	Acciones para direccionar riesgos y oportunidades.	Determinar los riesgos y oportunidades que deben ser dirigidas a:	Asegurar que el sistema de gestión puede lograr el (los) resultado (s) deseado (s).
				Prevenir o reducir los efectos no deseados.
				Lograr el mejoramiento continuo.
			La organización debe planear	Las acciones para dirigir estos riesgos y oportunidades.
				Integrar e implementar las acciones dentro de sus procesos de BCMS (véase numeral 8.1) y evaluar la eficacia de estas acciones.
	6.2	Objetivos de continuidad de negocio y planes para alcanzarlos	La alta dirección debe asegurar que los objetivos de la CN son establecidos y comunicados para las funciones y niveles pertinentes dentro de la organización	Ser coherentes con la política de Continuidad de Negocio.
				Tener en cuenta el nivel mínimo de productos y servicios que sea aceptable para que la organización logre sus objetivos.
				Ser medibles.
				Tener en cuenta los requisitos aplicables.
				Controlarse y actualizarse según corresponda.
	7	**RECURSOS**		
	7.1	Generalidades	La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el BCMS.	
	7.2	Competencia	La organización debe	Determinar las competencias necesarias del personal para hacer el trabajo que afecta su desempeño.
				Asegurarse que estas personas son competentes sobre la base de una educación adecuada, entrenamiento y experiencia.
				Si aplica tomar medidas para adquirir la competencia necesaria, y evaluar la eficacia de las medidas adoptadas.
				Mantener información documentada apropiada como evidencia de la competencia.
	7.3	Toma de conciencia	Las personas que realizan trabajos bajo el control de la	La política de Continuidad de Negocio
				Su contribución a la eficacia del BCMS, incluyendo los beneficios de la mejora del desempeño de la Gestión de Continuidad de Negocio.

	7.3	Toma de Conciencia	organización deben ser conscientes de:	Las implicaciones de las no conformidades con los requisitos del BCMS.
				Su propio rol ante un incidente.
	7.4	Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS	Sobre que comunicará.
				Cuando comunicar .
				Con quien comunicarse.
	7.5	Información documentada		
	7.5.1	Generalidades	El BCMS de la organización debe incluir:	
			- Información documentada y requerida por la norma.	
			- Información documentada que determine la organización.	
			La información de una organización difiere por:	
			- El tamaño de la organización.	
			- Complejidad de procesos.	
			- Competencia de personas.	
	7.5.2	Creación y actualización	Cuando se crea y actualiza la información documentada, la organización debe asegurar:	La identificación y descripción.
				Formato, medios de comunicación, revisión y aprobación adecuada y apropiada.
	7.5.3	Control de la información documentada	La información debe ser documentada y controlada para	Disponible y apropiada para el uso, donde y cuando sea necesario.
				Adecuadamente protegida (por ejemplo, de perdida de confidencialidad, uso inapropiado o perdida de integridad).
HACER	**8**	**OPERACIÓN**		
	8.1	Planificación y control.	La organización debe planear, implementar y controlar los procesos para cumplir los requisitos para ejecutar las acciones determinadas en el numeral 6.1	Establecer los criterios para esos procesos.
				Aplicar el control de estos procesos de acuerdo con los criterios.
				Mantener información documentada para demostrar que los procesos se han llevado a cabo como estaba Previsto.
	8.2	Análisis de impacto al negocio y valoración del riesgo.		

HACER	8.2.1	Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado para el análisis de impacto al negocio y valoración del riesgo	Establece el marco de la valoración, define los criterios y evalúa el impacto potencial de un incidente perjudicial.
				Toma en cuenta los requisitos legales y otros que la organización suscriba.
				Incluye un análisis sistemático, la priorización de los tratamientos de riesgo y sus costos relacionados.
				Define la salida necesaria del análisis de impacto al negocio y valoración del riesgo.
				Especifica los requisitos para que esta información se mantenga actualizada y confidencial.
	8.2.2	Análisis del impacto del negocio	La organización debe establecer, implementar y mantener un proceso de evaluación formal y documentado para determinar las prioridades de continuidad y recuperación, objetivos y metas .	La identificación de actividades que apoyan la prestación de bienes y servicios.
				La evaluación de los impactos en el tiempo de no realizar estas actividades.
				El establecimiento de plazos prioritarios para la reanudación de estas actividades a un nivel mínimo especificado aceptable, teniendo en cuenta los impactos de la no reanudación de ellas será inaceptable.
				La identificación de dependencias y recursos de apoyo para estas actividades, incluyendo proveedores, subcontratados, socios y otras partes interesadas pertinentes.
	8.2.3	Valoración del riesgo	La organización debe establecer, implementar y mantener un proceso formal de valoración del riesgo documentado que sistemáticamente identifica analiza y evalúa el riesgo de incidentes perjudiciales a la organización.	Identificar los riesgos de la interrupción de las actividades prioritarias de la organización y los procesos, sistemas de información, persona, bienes, proveedores y otros recursos que los apoyan.
				Analizar sistemáticamente el riesgo.
				Evaluar los riesgos relacionados con la interrupción que requieren tratamiento.
				Identificar tratamientos acordes con los objetivos de continuidad de negocio y de acuerdo con el apetito de riesgo de la organización.
	8.3	Estrategia de continuidad de negocio.		
	8.3.1.	Determinación y selección	Basarse en los resultados de los análisis de impacto al negocio y valoración del riesgo. (La determinación de la estrategia debe incluir la aprobación de marcos de prioridad de tiempo para la reanudación de las actividades).	Proteger las actividades prioritarias.
				Estabilizar, continuar, reanudar y recuperar las actividades priorizadas y sus dependencias y recursos de apoyo.
				Mitigar, responder y gestionar impactos.

HACER	8.3.2	Establecimiento de las necesidades de recursos	La organización debe determinar las necesidades de recursos para poner en práctica las estrategias seleccionadas. Los tipos de recursos considerados se incluyen, pero no se limitan a:	Las persona.
				La información y los datos.
				Los edificios, el ambiente de trabajo y servicios asociados.
				Instalaciones, equipos y consumibles.
				El sistema de información y la tecnología de comunicación.
				El transporte.
				La financiación.
				Socios y proveedores.
	8.3.3	Protección y mitigación.	Para los riesgos identificados que requieren tratamiento la organización debe considerar medidas proactivas que:	Reduzcan la probabilidad de interrupción.
				Acorten el período de interrupción.
				Limiten el impacto de la interrupción de los productos clave de la organización y servicios.
	8.4	Establecer e implementar procedimientos de continuidad de negocio.		
	8.4.1	Generalidades	Establecer e implementar procedimientos de continuidad de negocio.	Establecer un protocolo de comunicaciones interno y externo adecuado.
				Ser específicos con respecto a las medidas inmediatas que deben tomarse durante una interrupción.
				Ser flexibles para responder a amenazas imprevistas y las cambiantes condiciones internas y externas.
				Centrarse en el impacto de los eventos que podrían potencialmente interrumpir las operaciones.
				Ser desarrollados en base a los supuestos establecidos y el análisis de las interdependencias.
				Ser eficaces en la reducción de sus consecuencias a través de la aplicación de estrategias apropiadas de mitigación.
	8.4.2	Estructura de respuesta ante incidentes	La estructura de la respuesta debe:	Identificar los umbrales de los efectos que justifiquen la iniciación de la respuesta formal.
				Evaluar la naturaleza y el alcance de un incidente perjudicial y su impacto potencial.
				Activar una respuesta apropiada de Continuidad de negocio.
				Tener procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta.
				Tener los recursos disponibles para apoyar los procesos y procedimientos para manejar un incidente perjudicial para minimizar el impacto.

HACER				Comunicarse con las partes interesadas y las autoridades, así como los medios de comunicación.
	8.4.3	Advertencia y comunicación.	La organización debe establecer, implementar y mantener procedimientos:	La detección de un incidente.
				El seguimiento regular de un incidente.
				La comunicación interna dentro de la organización y recibir, documentar y responder a la comunicación de las partes interesadas.
				Recibir, documentar y responder a cualquier sistema de alerta de riesgo a nivel nacional o regional o su equivalente.
				Asegurar la disponibilidad de los medios de comunicación durante un incidente perjudicial.
				Facilitar la comunicación estructurada con los servicios de emergencia.
				Registrar la información vital sobre el incidente, las medidas adoptadas y las decisiones tomadas, y lo siguiente será considerado e implementado, donde aplique.
	8.4.4	Planes de continuidad de negocio	La organización debe tener procedimientos documentados para restaurar y retomar las actividades de negocio, de las medidas temporales adoptadas para soportar las necesidades normales del negocio después de un incidente.	
			Los planes de continuidad deben tener colectivamente:	Un proceso para la activación de la respuesta.
				Los detalles para gestionar las consecuencias inmediatas de un incidente perjudicial teniendo en cuenta:
				- El bienestar de los individuos.
				- Las opciones estratégicas, tácticas y operativas para la respuesta a la interrupción.
				- La prevención de la pérdida o no disponibilidad de las actividades prioritarias.
				La información detallada sobre cómo y bajo qué circunstancias la organización se comunicará con los empleados y sus familiares las partes interesadas claves y los contactos de emergencia.
				Cómo la organización va a continuar o recuperar sus actividades prioritarias dentro de los plazos predeterminados.
				Los detalles de la respuesta de la organización de los medios de comunicación a raíz de un incidente, incluyendo:
				- Estrategia de comunicación.
				- La interfaz seleccionada con los medios de comunicación.
				- Guía o plantilla para la redacción de una declaración para los medios de comunicación.

HACER	8.4.4	Planes de continuidad de negocio	Los planes de continuidad deben tener colectivamente:	-Portavoces apropiados.
				Un proceso para levantarse una vez que el incidente ha terminado. EL PLAN DEBE DEFINIR:
				- Propósito y alcance
				- Objetivos
				- Criterios y procedimientos de activación
				- Procedimientos de implementación
				- Roles responsabilidades y autoridades
				- Requisitos y procedimientos de comunicación
				- Interdependencias internas y externas y las interacciones
				- Necesidades de recursos y
				- Flujo de información y procesos de documentación
	8.4.5	Recuperación	La organización debe tener procedimientos documentados para restaurar y retornar las actividades de negocio, de las medidas temporales adaptadas para soportar las necesidades normales del negocio después de un incidente.	
	8.5	Ejercicios y pruebas	La organización debe hacer ejercitar y probar sus procedimientos de continuidad de negocio para asegurar que sean compatibles con sus objetivos de continuidad de Negocio.	Sean consistentes con el alcance y los objetivos del BCMS.
				Se basen en escenarios apropiados que están bien planificados, con objetivos claramente definidos.
				Tomen en conjunto con el tiempo validado la totalidad de los acuerdos de continuidad de negocio, involucrando las partes interesadas pertinentes.
				Reduzcan al mínimo el riesgo de interrupción de las operaciones.
				Produzcan formalmente, después del ejercicio, informes que contengan los resultados, recomendaciones y acciones a implementar.
				Revisen en el contexto de la promoción de la mejora continua.
				Se lleven a cabo a intervalos planificados, y cuando hay cambios significativos dentro de la organización o el medio ambiente en el que opera.
VERIFICAR	**9**	**EVALUACIÓN DE DESEMPEÑO**		
	9.1	Seguimientos, Medición, Análisis y evaluación.		
	9.1.1	Generalidades	La organización debe determinar:	Que necesita ser monitoreado y medido.
				Los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar la validez de los resultados.

VERIFICAR	9.1.1	Generalidades	La organización debe determinar:	Cuándo el seguimiento y la medición se llevarán a cabo.
				Cuándo los resultados del seguimiento y medición deben ser analizados y evaluados.
			La organización debe mantener información documentada como evidencia de los resultados.	
			La organización debe evaluar el desempeño del BCMS y su eficacia.	
			Además, la organización debe:	
			- Tomar acciones cuando sea necesario para hacer frente a las tendencias adversas o resultados antes de una no conformidad, y	
			- conservar la información documentada pertinente como evidencia los resultados.	
			Los procedimientos para seguimiento del desempeño deben proveer:	
			- El establecimiento de indicadores de desempeño adecuados a las necesidades de la organización,	
			- El seguimiento de la medida en que se cumplan las políticas de Continuidad de Negocio de la organización, los objetivos y metas.	
			- El desempeño de los procesos, procedimientos y funciones que protegen sus actividades prioritarias	
			- El control del cumplimiento con esta norma y los objetivos de continuidad de negocio,	
			- El seguimiento de la evidencia histórica de los resultados deficientes del desempeño del BCMS.	
			- El registro de datos y los resultados de seguimiento y medición para facilitar las acciones correctivas tomadas.	
	9.1.2	Evaluación de los procedimientos de continuidad de negocio		La organización debe llevar a cabo evaluaciones de sus procedimientos de Continuidad de Negocio y capacidades para asegurar su continua adecuación, idoneidad y eficacia.
				Las evaluaciones deben llevarse a cabo a través de revisiones periódicas, ejercicios, pruebas, reportes después de incidentes y evaluaciones de desempeño, los cambios significativos que surgen deben ser reflejados en el procedimiento de manera oportuna.
				Se debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentarios, mejores prácticas industriales, y la conformidad con su propia política y objetivos de continuidad de negocio.
				La organización debe llevar a cabo evaluaciones e intervalos planificados cuando se produzcan cambios significativos.

VERIFICAR	9.2	Auditoria interna	La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el BCMS	Se ajusta a:
				- Los requisitos propios de la organización para su BCMS
				- Los requisitos de esta norma.
				Es eficazmente implementado y mantenido
				La organización debe:
				- Planear establecer implementar y mantener un programa de auditoría incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y resultados. Los programas de auditoría deben tener en consideración la importancia de los procesos y de los resultados de auditorías anteriores.
				Definir los criterios de auditoría y el alcance de cada una.
				Seleccionar auditores y gestionar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría.
				Garantizar que los resultados de auditoría son reportados a la dirección.
				Mantener información documentada como evidencia de la implementación del programa de auditoría y de sus resultados.
	9.3	Revisión por la dirección	La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para asegurar su continua idoneidad, adecuación y eficacia. (La revisión por la dirección debe incluir la consideración de):	El estado de las acciones de las revisiones por la dirección previas.
				Los cambios en los asuntos internos y externos que son pertinentes para el BCMS.
				Información sobre el desempeño de Continuidad de Negocio, incluyendo las tendencias en:
				- Las no conformidades y acciones correctivas.
				- El seguimiento y la evaluación de resultados de la medición.
				- Resultado de la auditoría.
				Las oportunidades de mejora continua.
				Las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo:
				- La necesidad de cambios en el BCMS, incluyendo la política y los objetivos.
				- Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique.
				-Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS.

VERIFICAR	9.3	Revisión por la dirección	La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para asegurar su continua idoneidad, adecuación y eficacia. (La revisión por la dirección debe incluir la consideración de):	- El estado de acciones correctivas.
				- Los resultados de los ejercicios y pruebas.
				- Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior.
				- Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS.
				- La adecuación de la política.
				- Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales.
				- Buenas prácticas y guías emergentes.
				Variaciones en el alcance del BCMS.
				Mejoramiento de la eficacia del BCMS.
				Actualización de la valoración del riesgo, BIA, planes de continuidad de negocio, y procedimientos relacionados.
				Modificación de los procedimientos y controles para responder a los eventos internos o externos que pueden afectar al BCMS, incluidos los cambios;
				- Los requisitos del negocio y operacionales.
				- Reducción de riesgos y requisitos de seguridad.
				- Condiciones y procesos de operación.
				- Requisitos legales y reglamentarios.
				- Obligaciones contractuales.
				- Los niveles de riesgo y/o criterios de aceptación de riesgos.
				- Recursos necesarios.
				- La financiación y las necesidades presupuestarias.
				Como la eficacia de los controles son medidas.
			La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. La organización debe:	- Comunicar los resultados de examen de la gestión de las partes interesadas y pertinentes.
				- Tomar las medidas apropiadas en relación con esos resultados.

ACTUAR	**10**	**MEJORA**		
	10.1	No conformidad y acción correctiva	Cuando ocurra una no conformidad, la organización debe:	Identificar la no conformidad.
				Responder a las no conformidades, y, cuando aplique:
				- Tomar medidas para controlarlas y corregirlas.
				- Tratar con las consecuencias.
				Evaluar la necesidad de adoptar medidas para eliminar las causas de la no conformidad, para que así no se repita o se produzca en otra parte, incluyendo:
				- La revisión de las no conformidades.
				- La determinación de las causas de no conformidades.
				- La determinación de no conformidades similares existentes, o que potencialmente pudieran ocurrir.
				- La evaluación de la necesidad de acciones correctivas para asegurar que las no conformidades no se repitan o se produzcan en otros lugares.
				- La determinación e implementación de las acciones correctivas necesarias.
				- La revisión de la eficacia de cualquier acción correctiva tomada.
				- La elaboración de cambios al BCMS, si es necesario.
				Implementar cualquier acción requerida.
				Revisar la eficacia de cualquier acción tomada.
				Hacer los cambios al BCMS, si es necesario.
	10.2	Mejora continua	La organización debe mejorar continuamente la idoneidad, adecuación o eficacia del BCMS.	

Fuente: Elaboración de los autores, adaptada de la Norma Técnica Colombiana NTC 5722 Sistemas de gestión de continuidad de Negocio Requisitos.

5.2.3. Generación del Análisis GAP

Se realiza el análisis GAP tomando como insumo el manual “Sistema de gestión de Continuidad del Negocio” desarrollado por la entidad bancaria y se contrasta contra la norma NTC 5722 desde el numeral 4 al numeral 10.

Ver Anexo A.

5.3. FASE 3: VERIFICACIÓN DEL PRODUCTO

5.3.1. Generación de Recomendaciones de Fortalecimiento

En base al análisis GAP se desarrollan las recomendaciones de fortalecimiento así:

Tabla 7. Recomendaciones de fortalecimiento

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Planear	Contexto de la organización	4.1	Descripción de la organización y su contexto.	La organización debe identificar y documentar el apetito de riesgo de la organización.	En el manual No se hace referencia el apetito de riesgo del Banco	Para la generación del BIA por inherencia en su elaboración el banco debe tener claro el apetito de riesgo, pero en el manual no se nombra el apetito de riesgo en el proceso de elaboración, por lo tanto es necesario que en el manual se encuentre la identificación del apetito de riesgo y que esta identificación mencione la necesidad de estar debidamente documentada.
		4.1	Descripción de la organización y su contexto.	Al establecer el contexto, la organización debe establecer criterios de riesgo, teniendo en cuenta el apetito de riesgo.	En el manual No se hace referencia el apetito de riesgo del Banco	Los criterios o factores de riesgo mencionados en el manual no se está teniendo en cuenta que para establecerlos se está teniendo en cuenta el apetito de riesgo de la organización, por este motivo es importante formalizas dentro del manual el apetito de riesgo como factor fundamental en la instauración de los criterios de riesgo de continuidad del Banco.
	Recursos	7.3	Toma de conciencia	Las personas que realizan trabajos bajo el control de la organización deben ser conscientes de las implicaciones de las no conformidades con los requisitos del BCMS.	No se hace referencia en el documento a las implicaciones de las no conformidades con los requisitos del BCMS.	Dentro de los programas de sensibilización, formación y divulgación debe incluirse un aparte a nivel del plan de sensibilización y divulgación que indique la necesidad de establecer los riesgo e impactos de no gestionar los posibles hallazgos realizados por los entes de control, y/o las oportunidades de mejora identificadas por las pruebas de continuidad hechas a las estrategias y planes, realizadas por los encargados del proceso junto con el responsable asignado por el área de continuidad. Se debe incluir en las responsabilidades y roles de los diferentes involucrados en los BCMS del Banco labores asociadas a los ajustes de los BCMS. Se debe incluir en las responsabilidades y roles de los diferentes involucrados en los BCMS del Banco labores asociadas a los ajustes de los BCMS.

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Planear	Recursos	7.4	Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS sobre que comunicará.	En el manual no se especifica el contexto de lo que puede comunicarse en caso de ejecución del plan de comunicación de crisis.	Se debe ajustar el objetivo del plan de comunicación de crisis, y aclarar que el plan dará los lineamientos de lo que se comunicará al momento de la crisis.
		7.4	Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS sobre cuando se comunicara.	En el manual no se especifican los tiempos de comunicación interna y externa en caso de ejecución del plan de comunicación de crisis.	El manual establece el nivel de comunicación, los roles y las responsabilidades de quienes intervienen en el plan de comunicación de crisis, pero se debe formalizar el responsable de señalar los momentos en los que se emitirán las diferentes comunicaciones al interior del banco, los clientes, y autoridades pertinentes.
		7.5,2	Información documentada, creación y actualización.	Cuando se crea y actualiza la información documentada, la organización debe asegurar formatos, medios de comunicación, revisión y aprobación adecuada y apropiada.	En el documento no se especifican los Formatos de creación y actualización, medios de comunicación de los documentos, revisión y aprobación de la información documentada.	En el manual se especifican los diferentes formatos utilizados en el desarrollo e implementación de continuidad de negocio, incluso los establecidos para documentar los hallazgos en las revisiones generadas y las oportunidades de mejora encontradas, por lo tanto, se recomienda identificar en la "Tabla 2. Tareas de desarrollo e implementación de Continuidad de Negocio" las condiciones particulares que deben tener como: - Identificación y descripción - Medio de comunicación (papel o electrónico). - Medio de comunicación (papel o electrónico). - Revisión, y aprobación adecuada y apropiada.
		7.5,3	Información documentada, control de la información documentada.	La información debe ser documentada y controlada, para estar adecuadamente protegida (ejemplo; perdida de confidencialidad, uso inapropiado o perdida de integridad).	En el manual se hace énfasis en la documentación de cada proceso y plan, pero no se indica la protección de la confidencialidad, perdida de integridad, o el uso inapropiado.	Dentro del manual debe especificarse en sus diferentes instancias, la necesidad de mantener confidencialidad manejada al interior del Banco. Y especificar que la documentación generada en los diferentes momentos de la continuidad del negocio debe estar adecuadamente protegida.

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Hacer	Operación	**8.2**	**Análisis de impacto al negocio y valoración del riesgo.**			
		8.2.1	Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado que tenga un análisis sistemático, Ya priorización de los tratamientos de riesgo y sus costos relacionados.	En el análisis de impacto al negocio BIA, se hace referencia al análisis sistemático y a la priorización de los tratamientos de riesgo, pero No se hace referencian los costos relacionados o donde revisarlos.	En el manual se refieren a los costos y gastos de la realización de pruebas, mantenimiento de estrategias, e implementación de nuevas estrategias de continuidad , dentro del aparte de recursos y presupuestos, pero debe incluirse también en el aparte de Análisis de Impacto del Negocio dentro del ejercicio del BIA los costos relacionados a las estrategias de tratamiento del riesgo.
		8.2.1	Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado que especifique los requisitos para que esta información se mantenga actualizada y confidencial.	En el documento se describen los requisitos para actualizar la información pero No se hace referencia el tipo de tratamiento de confidencialidad frente a la misma.	El manual es amplio y explícito en la necesidad de documentar los procesos, mantener actualizadas las diferentes estrategias de continuidad y propender por la disponibilidad de la información y los procesos, pero no existe referencias hacia la protección de la información, ni entrega los lineamientos necesarios de confidencialidad en la documentación generada de los BCMS. Dentro del manual debe involucrarse a nivel de metodología y procesos de continuidad del negocio, lineamientos dirigidos a la confidencialidad de la información y toda documentación generada en los diferentes niveles de los planes de continuidad
		8.2.3	Valoración del riesgo	La organización tener un proceso formal de evaluación de riesgo documentado, Identificando tratamientos acordes con los objetivos de continuidad de negocio y de acuerdo con el apetito de riesgo de la organización.	En el manual No se hace referencia el apetito de riesgo del Banco	El banco necesita planear sus estrategias de acuerdo a sus capacidades, necesidades y contexto, desarrollando así un marco de referencia para que la toma de decisiones este dentro estos parámetros, es decir que las decisiones sean un balance entre crecimiento y seguridad, este marco de referencia es el apetito de riesgo, pero en el manual no se nombra el apetito de riesgo en el proceso de elaboración, por lo tanto es necesario que en el aparte de definición y diseño de estrategias de respuesta se encuentre explícito el apetito de riesgo como

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
						base para la elaboración de los tratamientos de riesgo.
Hacer	Operación	8.4.2	Estructura de respuesta ante incidentes	La estructura de la respuesta debe evaluar la naturaleza y el alcance de un incidente perjudicial y su impacto potencial.	En la estructura de la respuesta no se hace referencia a la evaluación de la naturaleza, del alcance y del impacto potencial del incidente, lo cual puede conllevar a la subvaloración del incidente por parte de los interesados.	En el manual, en la metodología en el aparte de Definición de planes de respuesta y manejo de crisis, debe incluirse en el alcance del plan de administración de crisis como alcance la evaluación de la naturaleza, alcance de un incidente y su impacto potencial.
		8.4.4	Planes de continuidad de negocio	Los planes de continuidad deben tener colectivamente: Un proceso para levantarse una vez que el incidente ha terminado. EL PLAN DEBE DEFINIR: - Propósito y alcance - Objetivos - Criterios y procedimientos de activación - Procedimientos de implementación - Roles responsabilidades y autoridades - Requisitos y procedimientos de comunicación - Interdependencias internas y externas y las interacciones - Necesidades de recursos y - Flujo de información y procesos de documentación	No se evidencia en el documento referencia al proceso a seguir para levantar el BCP una vez haya finalizado el incidente en la organización, lo cual puede provocar desarticulación de los procesos a realizar.	En el manual, en la metodología en el aparte de Definición de planes de respuesta y manejo de crisis, debe crearse un plan o incluir dentro de uno existente un proceso en el que se detalle, el paso a seguir una vez el incidente ha terminado, que incluya: - Propósito y alcance - Objetivos - Criterios y procedimientos de activación - Procedimientos de implementación - Roles responsabilidades y autoridades - Requisitos y procedimientos de comunicación - Interdependencias internas y externas y las interacciones - Necesidades de recursos y - Flujo de información y procesos de documentación

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Verificar	Evaluación de desempeño	**9.1**	**Seguimientos, Medición, Análisis y evaluación.**			
		9.1,1	Generalidades	La organización debe determinar, que necesita ser monitoreado y medido.	En el plan se habla del monitoreo como responsabilidades de los comités al momento de presentarse un evento, pero no hace referencia al seguimiento de los procesos con el ánimo de establecer que debe ser monitoreado con el fin de ser sometidos a pruebas.	Se debe esclarecer dentro del manual en la metodología y los procesos de continuidad de negocio, las características de lo que será monitoreado y medido, con el ánimo de realizar las pruebas en un ambiente controlado sobre los procesos, que se vean más afectados ante un evento.
		9.1,2	Evaluación de los procedimientos de continuidad de negocio	Evaluación de los procedimientos de continuidad de negocio, Se debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentario, mejores prácticas industriales, y la conformidad con su propia política y objetivos de continuidad de negocio.	No se hace referencia a la evaluación de la metodología utilizada frente a nuevos métodos, mejores prácticas, o nuevas normativa internacionales.	La metodología elaborada por el Banco requiere implementar revisiones anuales en búsqueda de una mejora continua en sus prácticas, en las que se contrate con buenas practicas a nivel gremial, con mejores prácticas industriales, o normas internacionales y sus actualizaciones. En el manual en procesos de gestión de continuidad del negocio, en el aparte de mejora continua debe incluirse en los catalizadores para el cambio la evaluación de la metodología contra mejores prácticas, y/o normativa internacional. Y en Metodología de continuidad del negocio, en el aparte de mantener estrategias, planes y documentación de continuidad incluir en las actividades de actualización, la revisión de la metodología frente a mejores prácticas, y/o normativa internacional.

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Verificar	Evaluación de desempeño	9.2	Auditoria interna	La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el BCMS, se ajusta a: - Los requisitos propios de la organización para su BCMS - Los requisitos de esta norma.	El documento no está ajustado totalmente a todos los requisitos solicitados en la norma NTC 5722	Como el manual no está basado en la ISO22301 (NTC 5722), se encontrarán no conformidades a la hora de la revisión por parte de la auditoria en el caso de compararlo con la norma internacional, por este motivo si se desea hacer la revisión contrastada con esta metodología, se deberá en primera instancia generar los cambios pertinentes para lograr que el manual se acoja a la ISO.
		9.3	Revisión por la dirección	La revisión por la dirección debe incluir la consideración Información sobre el desempeño de Continuidad de Negocio, incluyendo las tendencias en: - Las no conformidades y acciones correctivas. - El seguimiento y la evaluación de resultados de la medición. - Resultado de la auditoria	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN.	Establecer dentro del manual en la respuesta o proceso que debe hacerse por parte de las directivas ante la presentación de hallazgos de los entes de control, y el seguimiento y evaluación de los resultados de la medición.

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Verificar	Evaluación de desempeño	9.3	Revisión por la dirección	Las revisiones por la dirección deben considerar el desempeño de la organización (Ver comparativo aparte 9.1)	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN .	En el manual se debe incluir que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique. - Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas. - Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes.
		9.3	Revisión por la dirección	Variaciones en el alcance del BCMS	No existe referencias en el manual sobre la medición de la eficacia de los controles por parte de la alta dirección.	Establecer o especificar que en las revisiones generadas por la alta dirección deben incluirse decisiones relacionadas con las variaciones en el alcance de los BCMS, el mejoramiento de la eficacia de los BCMS y la medición de la eficacia de los controles.
		9.3	Revisión por la dirección	Mejoramiento de la eficacia del BCMS	No existen en el manual referencias a la documentación generada por la alta dirección frente a la revisión realizada por los entes de control.	

ISO 22301 / NTC 5722					Hallazgo	Recomendaciones
		Aparte	Sección	Descripción		
Verificar	Evaluación de desempeño	9.3	Revisión por la dirección	Como la eficacia de los controles son medidas.	No se hace referencia en el manual sobre la medición de la eficacia de los controles por parte de la alta dirección, lo cual puede provocar el desconocimiento del nivel en el cual las actividades planeadas son realizadas y los resultados planeados son alcanzados.	Incluir o especificar que en las revisiones generadas por la alta dirección deben incluirse decisiones relacionadas con las variaciones en el alcance de los BCMS, el mejoramiento de la eficacia de los BCMS y la medición de la eficacia de los controles.
		9.3	Revisión por la dirección	La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. La organización debe: - Comunicar los resultados de examen de la gestión de las partes interesadas y pertinentes. - Tomar las medidas apropiadas en relación con esos resultados.	No se hace referencia en el manual a la documentación generada por la alta dirección frente a la revisión realizada y a las medidas tomadas con base a los resultados, lo cual puede provocar incoherencias entre las medidas tomadas por la alta dirección y los intereses de las partes.	En el manual se debe incluir la necesidad de documentar la revisión efectuada por la alta dirección a la continuidad del negocio, y referir la documentación que se generará para la gestión de las partes interesadas, respecto a: - La comunicación de los resultados de examen de la gestión de las partes interesadas y pertinentes. - Tomar las medidas apropiadas en relación con esos resultados.
Actuar	Mejora	10.1	No conformidad y acción correctiva	Cuando ocurra una no conformidad, la organización debe revisar la eficacia de cualquier acción tomada.	No se hace referencia en el manual sobre la medición de la eficacia de cualquier acción tomada frente a una no conformidad, lo cual puede provocar el desconocimiento del nivel en el cual las actividades planeadas son realizadas y los resultados planeados son alcanzados.	Se debe incluir dentro del manual en el aparte de - Proceso de gestión continuidad del negocio referido a acciones correctivas - La revisión de la eficacia de las acciones tomadas para solventar las no conformidades encontradas. Adicional a lo mencionado se recomienda la creación de un indicador que identifique la eficacia de los controles implementados sobre las no conformidades encontradas.

Fuente: Elaboración de los autores, adaptada de la Norma Técnica Colombiana NTC 5722 Sistemas de gestión de continuidad de Negocio Requisitos y el manual de Sistema de Gestión de Continuidad del Negocio de la entidad bancaria.

6. PRODUCTOS A ENTREGAR

Análisis GAP, Documento con recomendaciones de fortalecimiento, Documento de proyecto de grado para entrega a la universidad, Artículo en formato IEEE para entrega a la universidad.

7. ENTREGA DE RESULTADOS E IMPACTOS

7.1. ENTREGA DE RESULTADOS E IMPACTOS FASE 1

Se realizó un análisis del contexto interno de la organización de acuerdo a la información recopilada. Al respecto se realizó una caracterización del entorno, teniendo en cuenta los elementos que intervienen en el comportamiento de la entidad bancaria y que son la base para las otras etapas propuestas en este proyecto de investigación. Dado lo anterior se evidencia que la entidad tiene una buena oportunidad para evaluar una metodología de un BCP vigente, ajustado al tamaño de sus procesos y número de sucursales, y por ser un BCP con opciones de mejora debido a que su metodología de creación no está basada estrictamente en un estándar internacional.

7.2. ENTREGA DE RESULTADOS E IMPACTOS FASE 2

Se realiza el análisis GAP de los controles establecidos en el BCP actual de la entidad bancaria frente a las recomendaciones dadas por la norma NTC 5722 con base al ciclo PHVA, el cual arroja que el porcentaje más bajo en nivel de cumplimiento de acuerdo al contraste, es el "**Planear**" en el **ítem** de **recursos** con un **70.59%** y el "**verificar**" para el **ítem** de **evaluación de desempeño** con un **68.97%,** en cuanto al porcentaje más alto está en el "**Planear**" para los **ítems** de **Liderazgo y Planificación** con el **100%** de cumplimiento.

Tabla 8. Resultados análisis GAP fase3.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Apartе	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
PLANEAR	4	Contexto de la organización	4.1 Descripción de la organización y su contexto.	La organización debe identificar y documentar el apetito de riesgo de la organización.	88,24%	No se hace referencia en el documento acerca de la identificación y documentación del apetito de riesgo del Banco, el cual les permitirá determinar el nivel de riesgo que puede asumir, mitigar o transferir la organización.
			4.1 Descripción de la organización y su contexto.	Al establecer el contexto, la organización debe establecer criterios de riesgo, teniendo en cuenta el apetito de riesgo.		No se hace referencia en el documento acerca del establecimiento de criterios de riesgo ya que en el documento no se está identificando y documentando el apetito de riesgo.
	5	Liderazgo			100%	
	6	Planificación			100%	
	7	Recursos	7.3 Toma de conciencia	Las personas que realizan trabajos bajo el control de la organización deben ser conscientes de las implicaciones de las no conformidades con los requisitos del BCMS.	70,59%	No se hace referencia en el documento a las implicaciones de las no conformidades con los requisitos del BCMS esto acarrearía que el personal reincida en las malas prácticas desarrolladas provocando la aparición de nuevos incidentes .
			7.4 Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS sobre que comunicará.		En el manual no se especifican los parámetros de comunicación en caso de ejecución del plan de comunicación de crisis, lo que conllevaría a la divulgación de información no autorizada.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Apartе	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
PLANEAR	7	Recursos	7.4 Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS sobre cuando se comunicara.	70.59%	En el manual no se especifican los tiempos de comunicación interna y externa en caso de ejecución del plan de comunicación de crisis lo que puede producir información errónea o malintencionada al interior de la organización, la cual puede ser comunicada de la misma manera a los usuarios..
			7.5.2 Creación y actualización	Cuando se crea y actualiza la información documentada, la organización debe asegurar formatos, medios de comunicación, revisión y aprobación adecuada y apropiada.		En el documento no se especifican los formatos de creación y actualización, medios de comunicación de los documentos, revisión y aprobación de la información documentada, lo cual conllevaría a procesos no formalizados e informalidad en las líneas de comunicación.
			7.5.3 Control de la información documentada	La información debe ser documentada y controlada, para estar adecuadamente protegida (por ejemplo, de perdida de confidencialidad, uso inapropiado o perdida de integridad).		En el plan se hace énfasis en la documentación de cada proceso y plan, pero no se indica la protección de la confidencialidad, pérdida de integridad, o el uso inapropiado, lo cual puede llevar a divulgación de información confidencial o controlada, pérdida o adulteración de esta.
HACER	8	Operación	8.2.1 Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado que tenga un análisis sistemático, la priorización de los tratamientos de riesgo y sus costos relacionados.	90,63%	En el análisis de impacto al negocio (BIA), se hace referencia al análisis sistemático y a la priorización de los tratamientos de riesgo pero no se hace referencia a los costos relacionados o donde revisarlos, lo que conlleva a desconocer el costo financiero del impacto.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Aparte	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
HACER	8	Operación	8.2.1 Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado que especifique los requisitos para que esta información se mantenga actualizada y confidencial.	90.63%	En el documento se describen los requisitos para actualizar la información pero no se hace referencia al tipo de tratamiento de confidencialidad frente a la misma, lo que puede acarrear que la información sensible sea de conocimiento público.
			8.2.3 Valoración del riesgo	La organización debe establecer, implementar y mantener un proceso formal de valoración del riesgo documentado que identifique tratamientos acordes con los objetivos de continuidad de negocio y de acuerdo con el apetito de riesgo de la organización.		No se hace referencia en el documento acerca de la identificación y documentación del apetito de riesgo del Banco por lo cual no están identificados los posibles tratamientos acordes con los objetivos de continuidad del negocio, esto conlleva a errores o imprecisiones en la cuantificación del impacto sobre los objetivos de negocio..
			8.4.2 Estructura de respuesta ante incidentes	La estructura de la respuesta debe evaluar la naturaleza y el alcance de un incidente perjudicial y su impacto potencial.		En la estructura de la respuesta no se hace referencia a la evaluación de la naturaleza, del alcance y del impacto potencial del incidente, lo cual puede conllevar a la subvaloración del incidente por parte de los interesados.
			8.4.4 Planes de Continuidad de Negocio	Los planes de continuidad deben tener colectivamente los detalles de la respuesta de la organización de los medios de comunicación a raíz de un incidente, incluyendo: - Estrategia de comunicación. - La interfaz seleccionada con los medios de comunicación. - Guía o plantilla para la redacción de una declaración para los medios de comunicación. -Portavoces apropiados.		En el documento no hay referencia en la respuesta de la organización en un incidente en cuanto a la estrategia, la interfaz y la guía o plantilla para la declaración a los medios de comunicación, lo cual puede provocar fallas en el control de la información divulgada.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Aparte	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
HACER	8	Operación	8.4.4 Planes de Continuidad de Negocio	Los planes de continuidad deben tener colectivamente un proceso para levantarse una vez que el incidente ha terminado. EL PLAN DEBE DEFINIR: - Propósito y alcance - Objetivos - Criterios y procedimientos de activación - Procedimientos de implementación - Roles responsabilidades y autoridades - Requisitos y procedimientos de comunicación - Interdependencias internas y externas y las interacciones - Necesidades de recursos y - Flujo de información y procesos de documentación	**90.63%**	No se evidencia en el documento referencia al proceso a seguir para levantar el BCP una vez haya finalizado el incidente en la organización, lo cual puede provocar desarticulación de los procesos a realizar.
VERIFICAR	9	Evaluación de Desempeño	9.1.1 Generalidades	La organización debe determinar que necesita ser monitoreado y medido.	**68.97%**	En el plan se habla del monitoreo como responsabilidades de los comités al momento de presentarse un evento, pero no hace referencia al seguimiento de los procesos con el ánimo de establecer que debe ser monitoreado con el fin de ser sometido a pruebas.
			9.1.2 Evaluación de procedimiento de Continuidad de Negocio	Se debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentarios, mejores prácticas industriales, y la conformidad con su propia política y objetivos de continuidad de negocio.		En el documento no se hace referencia a la evaluación de la metodología utilizada frente a nuevos métodos, mejores prácticas, o nuevas normativas, lo cual puede provocar desactualización del BCP en cuanto a requisitos legales y mejores prácticas de operación.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Aparte	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
VERIFICAR	9	Evaluación de Desempeño	9.2 Auditoria Interna	La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el BCMS, se ajusta a los requisitos de esta norma.	68.97%	El documento no está ajustado en su totalidad a todos los requisitos solicitados por la norma NTC 5722, lo cual puede provocar incumplimiento en caso de un eventual proceso de certificación. Adicionalmente pueden existir procesos, aspectos de la organización y partes interesadas que no hayan sido contempladas en el sistema de Gestión de Continuidad del Negocio.
			9.3 Revisión por la Dirección	Información sobre el desempeño de Continuidad de Negocio, incluyendo las tendencias en: - Las no conformidades y acciones correctivas. - El seguimiento y la evaluación de resultados de la medición. - Resultado de la auditoría.		En el documento no se hace referencia a la revisión de la dirección del desempeño de la continuidad del negocio, en cuanto a las tendencias de las no conformidades y acciones correctivas, así como el seguimiento, la evaluación y resultados de la auditoría, lo cual puede provocar desconocimiento del actual estado del desempeño y nivel de avance del SGCN.
			9.3 Revisión por la Dirección	Las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique. -Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas.		Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 las acciones de la alta dirigencia, en cuanto a la revisión del SGCN cuando existen cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluyen que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Aparte	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
				- Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes.		-Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas. - Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes. Generando una posible falta de gestión de las partes interesadas respecto a los ajustes propios de los BCMS, considerados por la revisiones de las mediciones efectuadas por parte de las altas directivas.
VERIFICAR	9	Evaluación de Desempeño	9.3 Revisión por la Dirección	Variaciones en el alcance del BCMS	**68.97%**	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluye que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en las variaciones en el alcance del BCMS, Que puede conllevar a acciones ineficaces para el control de un evento, puesto que se están dejando por nuevos procesos resultantes de las variaciones del negocio.

PHVA	ISO 22301 / NTC 5722				% cumplimiento	Hallazgos en el manual sistema de gestión de continuidad del negocio
	Aparte	Sección	Contexto	Descripción ISO 22301 / NTC 5722		
			9.3 Revisión por la Dirección	Mejoramiento de la eficacia del BCMS		Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluyen que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en el mejoramiento de la eficacia del BCMS, lo que conlleva a la ausencia de una búsqueda del mejoramiento continuo, y una contrariedad al énfasis dado por el mismo manual en el mejoramiento y mantenimiento de las estrategias de continuidad de negocio.
VERIFICAR			9.3 Revisión por la Dirección	La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para asegurar su continua idoneidad, adecuación y eficacia. (La revisión por la dirección debe incluir la consideración de) Como la eficacia de los controles son medidas.	68.97%	No se hace referencia en el manual sobre la medición de la eficacia de los controles por parte de la alta dirección, lo cual puede provocar el desconocimiento del nivel de avance de las actividades planeadas y realizadas y el nivel de avance de los resultados alcanzados.
			9.3 Revisión por la Dirección	La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. La organización debe: - Comunicar los resultados de examen de la gestión de las partes interesadas y pertinentes. - Tomar las medidas apropiadas en relación con esos resultados.		No se hace referencia en el manual a la documentación generada por la alta dirección frente a la revisión realizada y a las medidas tomadas con base a los resultados, lo cual puede provocar incoherencias entre las medidas tomadas por la alta dirección y los intereses de las partes.
ACTUAR	10	Mejora	10.1 No conformidad y acción correctiva	Cuando ocurra una no conformidad, la organización debe revisar la eficacia de cualquier acción tomada.	86%	No se hace referencia en el manual sobre la medición de la eficacia de cualquier acción tomada frente a una no conformidad, lo cual puede provocar el desconocimiento del nivel de avance de las actividades planeadas y el nivel de los resultados alcanzados.

Fuente: Elaboración de los autores, adaptada de la Norma Técnica Colombiana NTC 5722 Sistemas de gestión de continuidad de Negocio Requisitos y el manual de Sistema de Gestión de Continuidad del Negocio de la entidad bancaria.

7.3. ENTREGA DE RESULTADOS E IMPACTOS FASE 3

De acuerdo a los resultados del análisis GAP, se realizan las recomendaciones de fortalecimiento así:

Tabla 9. Número de recomendaciones elaboradas de acuerdo al análisis GAP

Ciclo PHVA	Sección	# de Controles	% De cumplimiento aplicando la NTC 5722
Planear	Contexto de la organización	2	88,24%
	Recursos	5	70,59%
Hacer	Operación	5	90,63%
Verificar	Evaluación de Desempeño	9	68,97%
Actuar	Mejora	1	85,71%

Fuente: Elaboración autores

Ver 5.3.1.Generación de Recomendaciones de Fortalecimiento

Se sugiere **dar prioridad** en el ciclo PHVA al componente de **verificar**, ya que según el análisis GAP realizado, este ítem es el que menor porcentaje de cumplimiento de la norma NTC 5722 tiene con un **68,97%** y mayor número de controles (9) por fortalecer en los siguientes aspectos:

Tabla 10. Priorización de fortalecimiento según ciclo PHVA

Ciclo PHVA	Sección de la norma	Descripción
Verificar	Evaluación de Desempeño / Generalidades	La organización debe determinar que necesita ser monitoreado y medido.
	Evaluación de Desempeño /Evaluación de los procedimientos de Continuidad de Negocio	Se debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentarios, mejores prácticas industriales, y la conformidad con su propia política y objetivos de continuidad de negocio.
	Evaluación de Desempeño / Auditoría Interna	La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el BCMS, se ajusta a los requisitos de esta norma.
	Evaluación de Desempeño / Revisión por la Dirección	Información sobre el desempeño de Continuidad de Negocio, incluyendo las tendencias en: - Las no conformidades y acciones correctivas. - El seguimiento y la evaluación de resultados de la medición. - Resultado de la auditoría.

Ciclo PHVA	Sección de la norma	Descripción
		Las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique. -Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas. - Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes.
		Variaciones en el alcance del BCMS
		Mejoramiento de la eficacia del BCMS
		La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para asegurar su continua idoneidad, adecuación y eficacia. (La revisión por la dirección debe incluir la consideración de) Cómo la eficacia de los controles son medidas.
		La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. La organización debe: - Comunicar los resultados de examen de la gestión de las partes interesadas y pertinentes. - Tomar las medidas apropiadas en relación con esos resultados.

Fuente: Elaboración de los autores, adaptada de la Norma Técnica Colombiana NTC 5722 Sistemas de gestión de continuidad de Negocio Requisitos.

8. NUEVAS ÁREAS DE ESTUDIO

El paso a seguir con los resultados del trabajo, es realizar la implementación de las recomendaciones entregadas, ajustando el manual a nivel metodológico, de procesos, roles, responsabilidades, recursos y responsabilidades.

El trabajo está planteado como base para iniciar la revisión a nivel de áreas y procesos de la entidad bancaria, identificando a nivel individual cada BCMS creado con la metodología planteada en el manual de gestión de continuidad, y hacerle la revisión bajo los lineamientos de la ISO22301, junto con las recomendaciones entregadas. La implementación de estas recomendaciones busca encaminar a la entidad bancaria a la certificación del estándar internacional.

9. CONCLUSIONES

- La aplicación de las normas ISO permiten implementar en la entidad procedimientos que garanticen el buen funcionamiento de todas las áreas de la organización, propendiendo por la adopción de un enfoque basado en procesos cuando se desarrolla, implanta y mejora la eficacia de un sistema de gestión.

- La norma ISO22301 enfatiza la necesidad de comprender la organización, las necesidades de establecer políticas y objetivos de gestión de la continuidad del negocio, implementando controles y administrando la capacidad de toda la organización para gestionar incidentes disruptivos, dando seguimiento a la efectividad y desempeño del BCMS, buscando la mejora continua de su sistema por medio del monitoreo constante y la medición objetiva.

- Confrontar el manual de continuidad de negocio de la organización contra la norma, permitió evidenciar las oportunidades de mejora que presenta el manual, pero también logro demostrar que, pese a que el manual no está estructurado bajo los lineamientos de la normativa internacional, si cuenta con grandes similitudes en su composición y los apartes manejados se asemejan a los distintos componentes que tiene la ISO22301.

- Los resultados generados por el análisis GAP, permiten entregar recomendaciones para fortalecer el manual de continuidad de negocio del Banco, dando solidez a la respuesta ante incidentes a pequeña y gran escala que afecten de forma directa la prestación de los servicios.

- Según los resultados generados por el análisis GAP, nos permite evidenciar el porcentaje de cumplimientos del BCMS del banco frente a la norma ISO22301:

Aparte de la norma ISO22301/ NTC5722	Porcentaje de cumplimiento del BCMS del Banco frente a la norma
Contexto de la organización	88,24%
Recursos	70,59%
Operación	90,63%
Evaluación de Desempeño	68,97%
Mejora continua	85,71%
Porcentaje global de cumplimiento.	**80,83%**

- Según la confrontación realizada, se vislumbra que dentro del ciclo PHVA las oportunidades de mejora distribuyen así;
    - Planear 7 hallazgos
    - Hacer 5 hallazgos
    - Verificar 9 hallazgos
    - Actuar 1 hallazgos

- Según las oportunidades de mejora encontradas, se vislumbra que dentro del ciclo PHVA, el componente de la norma en el que se puede lograr un mayor ajuste dentro del manual es en el verificar, debido a la baja profundización que se hace a la evaluación de los procesos, responsabilidades y roles de la alta dirección respecto a la revisión de los BCMS.

10. BIBLIOGRAFÍA

Asobancaria. (24 de 09 de 2018). ¿El sector financiero está preparado ante el riesgo de un desastre natural? *Semana Económica, Edición 1155*, págs. 2 - 7. Recuperado el 26 de 09 de 2019. Obtenido de https://www.asobancaria.com/wp-content/uploads/1155.pdf

Asobancaria. (24 de 09 de 2018). ¿El sector financiero está preparado ante el riesgo de un desastre natural? *Semana economica, Edición 1155*, pág. 6. Recuperado el 11 de 09 de 2019. Obtenido de https://www.asobancaria.com/wp-content/uploads/1155.pdf

Asobancaria. (26 de 03 de 2019). Riesgo cibernético y el futuro de la estabilidad financiera.*Semana Economica,* Edición 1178, pág. 4. Recuperado el 24 de 03 de 2020, Obtenido de https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

BusinessContinuity - Perú. (09 07 2012). Antecedentes históricos de la Continuidad del Negocio. Recuperado el 24 de 09 de 2019. Obtenido de : https:// http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html.

Caracol Radio. (08 de 05 de 2019). Desastres naturales le han costado al país US$ 7.100 millones. Recuperado el 11 de 03 de 2020. Obtenido de https://caracol.com.co/radio/2019/05/08/economia/1557324643_909854.html

Congreso De La República de Colombia. (31 de 12 de 2008). Ley estatutaria 1266 de 2008. Recuperado el 11 de 10 de 2019. Obtenido de http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

Congreso de la República de Colombia. (18 de 10 de 2012). Ley estatutaria 1581 de 2012. Recuperado el 11 de 03 de 2020. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso De La República de Colombia. (18 de 10 de 2012). Ley estatutaria 1581 de 2012. Recuperado el 11 de 03 de 2020. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

DELGADILLO, D., FLORES, I., HERNÁNDEZ R., & SANDOVAL M. (2009). Propuesta de intervención para la continuidad de negocio en trámites y servicios electrónicos del Gobierno mexicano. México. Trabajo de Grado (Maestría en Dirección estratégica de tecnologías de la información y comunicación). Fondo de Información y Documentación para la Industria INFOTEC. Recuperado el 11 de 10 de 2019. Obtenido de http://infotec.repositorioinstitucional.mx/jspui/handle/1027/234

El Colombiano. (15 de 03 de 2018). Bancolombia presentó fallas a nivel nacional en pleno día de quincena. Recuperado el 26 de 09 de 2019. Obtenido de https://www.elcolombiano.com/antioquia/bancolombia-presenta-fallas-a-nivel-nacional-CJ8391620

Icontec. (2012). Norma Técnica Colombiana NTC 5722. En Sistemas de Gestión de Continuidad de Negocio _ Requisitos. Bogotá: Icontec. págs. 2-4

Icontec. (2012). Norma Técnica Colombiana NTC 5722. En Sistemas de Gestión de Continuidad de Negocio _ Requisitos. Bogotá: Icontec. pág. 2-5,6

Icontec. (2012). Norma Técnica Colombiana NTC 5722. En Sistemas de Gestión de Continuidad de Negocio _ Requisitos. Bogotá: Icontec. págs. 5,6

Icontec. (2012). Norma Técnica Colombiana NTC 5722. En Sistemas de Gestión de Continuidad de Negocio _ Requisitos. Bogotá: Icontec. pág. I

Icontec. (2012). Norma Técnica Colombiana NTC 5722. En Sistemas de Gestión de Continuidad de Negocio _ Requisitos. Bogotá: Icontec., págs. II, III

ISOTools. (18 08 2017). Sistema de Administración del Riesgo Operativo (SARO): ¿Cómo administrar los riesgos? Recuperado el 20 de 04 de 2020. Obtenido de https://www.isotools.com.co/sistema-administracion-del-riesgo-operativo-saro-administrar-los-riesgos/

La República. (18 de 09 de 2019). Fallas en cajeros y descuentos sin razón, entre las principales quejas de las tarjetas débito. Recuperado el 11 de 03 de 2020. Obtenido de https://www.larepublica.co/finanzas/fallas-en-cajeros-y-descuentos-sin-razon-quejas-de-las-tarjetas-debito-2909557

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (05 de 01 de 2009). Ley 1273 de 2009. Recuperado el 05 de 10 de 2019. Obtenido de https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MinTIC. (12 de 12 de 2014). Decreto número 2573 de 2014. Recuperado el 05 de 10 de 2019. Obtenido de https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

RCN Radio. (12 de 11 de 2019). Bancos podrían suspender atención por paro nacional. Recuperado el 11 de 03 de 2020. Obtenido de https://www.rcnradio.com/economia/bancos-podrian-suspender-atencion-por-paro-nacional

Revista Portafolio. (29 de 01 de 2019). El secuestro de información desangra a las empresas del país. Recuperado el 26 de 09 de 2019. Obtenido de https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

Rojas, J. (2017). Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del ecuador. Trabajo de Grado (Maestría en Gerencia de sistemas y de tecnologías de la información). Facultad de postgrados UDLA. Recuperado el 11 de 10 de 2019. Obtenido de http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

SISTESEG. (2020). Plan para la continuidad del negocio (BCP Y DRP ISO 22301). Recuperado el 04 de 03 de 2020. Obtenido de https://www.sisteseg.com/sindustrial.html

Superintendencia Financiera de Colombia. (19 de 03 de 1999). Circular Externa 004 de 1999. Recuperado el 05 de 10 de 2019. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/553/dPrint/1/c/00

Superintendencia Financiera de Colombia. (06 de 2007). Reglas relativas a la administración del riesgo operativo. Recuperado el 20 de 04 de 2020. Obtenido de https://fasecolda.com/cms/wp-content/uploads/2019/08/ce041-2007-anexo.pdf

Superintendencia Financiera de Colombia. (29 de 06 de 2007). Circular Externa 041 de 2007. Recuperado el 11 de 10 de 2019. Obtenido de https://www.superfinanciera.gov.co/publicacion/20068

Superintendencia Financiera de Colombia. (20 de 04 de 2009). Circular externa 038 de 2009. Recuperado el 05 de 10 de 2019. Obtenido de https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile22457&downloadname=ce038_09.doc

Superintendencia Financiera de Colombia. (29 de 03 de 2010). Circular Externa 008 de 2010. Recuperado el 05 de 10 de 2019. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20148/dPrint/1/c/20149

Superintendencia Financiera de Colombia. (04 de 10 de 2012). Circular Externa 042 de 2012. Recuperado el 10 Obtenido de 05 de 2019. de https://www.superfinanciera.gov.co/publicacion/20142

Superintendencia Financiera de Colombia. (05 de 06 de 2018). Circular Externa 007 de 2018. Recuperado el 03 de 24 de 2020. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Superintendencia Financiera de Colombia. (05 de 06 de 2018). Circular Externa 008 de 2018. Recuperado el 03 de 24 de 2020. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Superintendencia Financiera de Colombia. (10 de 09 de 2019). Informe de Operaciones Primer semestre 2019. Recuperado el 24 de 09 de 2019. Obtenido de https://www.superfinanciera.gov.co/publicacion/61066

TORRES, J., & VELASCO, H. (18 de 11 de 2014). Diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de bogotá. Bogotá. Trabajo de Grado (Pregrado Ingenieria de sistemas). *Repositorio universidad catolica de colombia*. Recuperado el 02 de 10 de 2019. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/1706/1/Trabajo%20de%20Investigacion%20BCP%20Hospitales%20de%20la%20Ciudad%20de%20Bogota.pdf

11. ANEXOS

Anexo A. Tabla_ Análisis GAP

Planear	
Hacer	
Verificar	
Actuar	

ISO 22301 / NTC 5722			
Aparte	**Sección**	**Descripción**	
4	**CONTEXTO DE LA ORGANIZACIÓN**		
4.1	Descripción de la organización y su contexto.	La organización debe identificar y documentar:	Los procesos de la organización, funciones, servicios, productos, asociaciones, cadenas de suministro, las relaciones con las partes interesadas, y el impacto potencial relacionado con un incidente perjudicial
			Las relaciones entre la política de continuidad de Negocio y objetivos de la organización y de otras políticas, como su estrategia de gestión de riesgo global
			Apetito de riesgo de la organización.

ASIMILACIÓN CON LA NORMA MANUAL SISTEMA DE GESTIÓN CONTINUIDAD DEL NEGOCIO					
Aparte	**Sección**	**Subsección**	**Aclaraciones**	**Hallazgo**	**%**
3.1 3.6	Principios y lineamientos Metodología de Continuidad del Negocio	3.6. 1 Entendimiento y perfil de negocio	Registros vitales	No aplica	**88,24%**
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.1 Planear la continuidad del negocio 3.6.3 Análisis de impacto al negocio – BIA	Registros vitales	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el documento acerca de la identificación y documentación del apetito de riesgo del Banco, el cual les permitirá determinar el nivel de riesgo que puede asumir, mitigar o transferir la organización.	

Aparte	Sección	Descripción	
		Al establecer el contexto, la organización debe:	Articular sus objetivos, incluidos los relativos a la Continuidad de Negocio.
			Definir los factores externos e internos que generan la incertidumbre que da lugar al riesgo.
			Establecer criterios de riesgo, teniendo en cuenta el apetito de riesgo.
			Definir el propósito del BCMS.
4.2	Entendiendo las necesidades y expectativas de las partes interesadas.		Generalidades
4.2.1	Generalidades	Cuando se establece un BCM la organización debe determinar:	Las partes interesadas que son pertinentes del BCMS
			Los requisitos de estas partes interesadas

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.1 Planear la continuidad del negocio a) Identificar necesidades en la continuidad de negocio en el Banco 3.6. 1 Entendimiento y perfil de negocio	No aplica	No aplica	
3.4 3.6	Proceso de gestión continuidad del negocio . Metodología de Continuidad del Negocio.	3.4.1 Planear la continuidad del negocio a) Identificar necesidades en la continuidad de negocio en el Banco. 3.6. 1 Entendimiento y perfil de negocio .	No aplica	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el documento acerca del establecimiento de criterios de riesgo ya que en el documento no se está identificando y documentado el apetito de riesgo.	
1 3.4 3.6	Objetivo . Proceso de Gestión de Continuidad del Negocio. Metodología de Continuidad del Negocio.	3.4..1 Planear la continuidad del negocio	No aplica	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.6. 1 Entendimiento y perfil de negocio	No aplica	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.6.1 Entendimiento y perfil de negocio	No aplica	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio. Metodología de	3.6.1 Entendimiento y perfil de negocio	No aplica	No aplica	

Aparte	Sección	Descripción	
4.2.2	Requisitos legales y reglamentarios		
4.3	Determinar el alcance del sistema de gestión.		
4.3.1	Generalidades	Se debe determinar el alcance del sistema de gestión.	
4.3.2	Alcance del BCMS	La organización debe:	Establecer las partes de la organización para ser incluidas en el BCMS
			Establecer los requisitos de BCMS, teniendo en cuenta la misión de la organización, los objetivos, las obligaciones internas y externas, y las responsabilidades legales y regulatorias
			identificar los productos, servicios y todas las actividades relacionadas con el alcance del BCMS.
			Tener en cuenta las necesidades de las partes interesadas y los intereses.
			Definir el alcance del BCMS en términos de y apropiado para el tamaño, la naturaleza y complejidad de la organización.
5	**LIDERAZGO**		
5.1	Generalidades.	Las personas de la alta dirección y otros roles directivos pertinentes de la organización deben demostrar liderazgo con respecto al BCMS.	

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	Continuidad del Negocio.				
3.1	Principios y Lineamientos	No aplica	No aplica	No aplica	
2	**Alcance**		No aplica	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio. Metodología de Continuidad del Negocio.	No aplica	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.7 Definir el personal responsable de dar la respuesta ante un evento o crisis	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.1 Entendimiento y perfil de negocio 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.1 Planear la continuidad del negocio 3.6.2 Evaluación de riesgos de continuidad		No aplica	
2	Alcance		No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.2	Gobierno de Continuidad del Negocio	3.2.1 Roles y responsabilidades	No aplica	No aplica	**100%**

Aparte	Sección	Descripción	
5.2	Compromiso de la alta dirección.	La alta dirección debe demostrar su liderazgo y compromiso: - Políticas y objetivos. - Integración . - Recursos. - Comunicación. - Resultados. - Mejora continua.	
		La alta dirección asegurar responsabilidades y autoridad. - Definición de criterios de riesgo. - Participando en pruebas. - Asegurar auditorías. - Mejora continua.	
5.3	Política.	La alta dirección debe establecer y comunicar una política de continuidad de negocio	Ser adecuada para el propósito de la organización
			Proporcionar el marco para establecer objetivos de Continuidad de Negocio
			Incluir un compromiso para satisfacer los requisitos aplicables
			Incluir un compromiso de mejora continua del BCMS
5.4	Roles, responsabilidades y autoridades.	La alta dirección debe asegurarse de que las responsabilidades y autoridades para	Asegurar que el sistema de gestión se establezca en conformidad con los requisitos de la norma.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.2	**POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO Versión 7 del 26/06/2019** Gobierno de la continuidad del negocio	3.2.1 Roles y responsabilidades	No aplica	No aplica	
3.2	**POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO Versión 7 del 26/06/2019** Gobierno de la continuidad del negocio	3.2.1 Roles y responsabilidades	No aplica	No aplica	
1	**POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO Versión 7 del 26/06/2019** Objetivos	1. Objetivos específicos	No aplica	No aplica	
1	**POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO Versión 7 del 26/06/2019** Objetivos	1. Objetivos específicos	No aplica	No aplica	
1	**POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO Versión 7 del 26/06/2019** Objetivos	1. Objetivos específicos	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
3.1	Principios y Lineamientos		No aplica	No aplica	

Aparte	Sección	Descripción	
		las funciones pertinentes se asignen y sean comunicadas.	Informar sobre el desempeño del BCMS a la alta dirección.
6	**PLANIFICACIÓN**		
6.1	Acciones para direccionar riesgos y oportunidades.	Determinar los riesgos y oportunidades que deben ser dirigidas a:	Asegurar que el sistema de gestión puede lograr el (los) resultado (s) deseado (s)
			Prevenir o reducir los efectos no deseados.
			Lograr el mejoramiento continuo.
		La organización debe planear	Las acciones para dirigir estos riesgos y oportunidades
			Integrar e implementar las acciones dentro de sus procesos de BCMS (véase numeral 8.1) y evaluar la eficacia de estas acciones
6.2	Objetivos de continuidad de	La alta dirección debe asegurar que los objetivos de la	Ser coherentes con la política de Continuidad de Negocio

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.2 3.4	Gobierno de Continuidad del Negocio Proceso de gestión continuidad del negocio	3.2.1 Roles y responsabilidades 3.4.3 Verificar y revisar la continuidad de negocio	No aplica	No aplica	
3.1 3.4	Principios y lineamientos Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio	No aplica	No aplica	**100%**
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.1 3.4 3.6	Principios y lineamientos Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.2 Evaluación de riesgos de continuidad 3.6.6 Definición de planes de respuesta y manejo de crisis	No aplica	No aplica	
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
1.	Objetivo	1. Objetivos específicos	No aplica	No aplica	

Aparte	Sección	Descripción		Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	negocio y planes para alcanzarlos	CN son establecidos y comunicados para las funciones y niveles pertinentes dentro de la organización	Tener en cuenta el nivel mínimo de productos y servicios que sea aceptable para que la organización logre sus objetivos.	3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.1 Planear la continuidad del negocio 3.6.2 Evaluación de riesgos de continuidad	No aplica	No aplica	
			Ser medibles	3.5	Métricas y medición de la gestión de continuidad del negocio	3.5.1 Medición de la cultura de continuidad	No aplica	No aplica	
			Tener en cuenta los requisitos aplicables	3.4	Proceso de gestión continuidad del negocio	3.4.1 Planear la continuidad del negocio a) Identificar necesidades en la continuidad de negocio en el Banco	No aplica	No aplica	
			Controlarse y actualizarse según corresponda	3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio	No aplica	No aplica	
7	**RECURSOS**								
7.1	Generalidades	La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el BCMS		3.3	Recursos y presupuesto		No aplica	No aplica	
7.2	Competencia	La organización debe	Determinar las competencias necesarias del personal para hacer el trabajo que afecta su desempeño.	3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.7 Definir el personal responsable de dar la respuesta ante un evento o crisis	No aplica	No aplica	
			Asegurarse que estas personas son competentes sobre la base de una educación adecuada, entrenamiento y experiencia.	3.3 3.6	Recursos y presupuesto Metodología de Continuidad del Negocio	3.6.8 Establecer el programa de sensibilización, formación y divulgación	No aplica	No aplica	**70,59%**
			Si aplica tomar medidas para adquirir la competencia necesaria, y evaluar la eficacia de las medidas adoptadas.	3.4	Proceso de gestión continuidad del negocio	3.4.1 Planear la continuidad del negocio 3.4.3 Verificar y revisar la continuidad de negocio	No aplica	No aplica	
			Mantener información documentada apropiada como evidencia de la competencia.	3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	

Aparte	Sección	Descripción	
7.3	Toma de conciencia	Las personas que realizan trabajos bajo el control de la organización deben ser conscientes de:	La política de Continuidad de Negocio
			Su contribución a la eficacia del BCMS, incluyendo los beneficios de la mejora del desempeño de la Gestión de Continuidad de Negocio.
			Las implicaciones de las no conformidades con los requisitos del BCMS.
			Su propio rol ante un incidente.
7.4	Comunicación	La organización debe determinar la necesidad de comunicación interna y externa del BCMS	Sobre que comunicará.
			Cuando comunicar
			Con quien comunicarse
7.5	Información documentada		

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.5.	Métricas y medición de la gestión de continuidad del negocio	3.5.1 Medición de la cultura de continuidad / C)Conciencia	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.8 Establecer el programa de sensibilización, formación y divulgación	No se hace referencia la contribución a la eficacia del BCMS	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el documento a las implicaciones de las no conformidades con los requisitos del BCMS esto acarrearía que el personal reincida en las malas prácticas desarrolladas provocando la aparición de nuevos incidentes .	
3.6	Metodología de Continuidad del Negocio	3.6.8 Establecer el programa de sensibilización, formación y divulgación		No aplica	
	No se evidencia en el documento	No aplica	Plan comunicación de crisis	En el manual no se especifican los parámetros de comunicación en caso de ejecución del plan de comunicación de crisis, lo que conllevaría a la divulgación de información no autorizada.	
	No se evidencia en el documento	No aplica	Plan comunicación de crisis	En el manual no se especifican los tiempos de comunicación interna y externa en caso de ejecución del plan de comunicación de crisis lo que puede producir información errónea o malintencionada al interior de la organización la cual puede ser comunicada de la misma manera a los usuarios.	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	Plan comunicación de crisis	No aplica	

Aparte	Sección	Descripción	
7.5.1	Generalidades	El BCMS de la organización debe incluir: - Información documentada y requerida por la norma. - Información documentada que determine la organización. La información de una organización difiere por: - El tamaño de la organización. - Complejidad de procesos. - Competencia de personas.	
7.5.2	Creación y actualización	Cuando se crea y actualiza la información documentada, la organización debe asegurar:	La identificación y descripción
			Formato, medios de comunicación, revisión y aprobación adecuada y apropiada.
7.5.3	Control de la información documentada	La información debe ser documentada y controlada para	Disponible y apropiada para el uso, donde y cuando sea necesario
			Adecuadamente protegida (por ejemplo, de perdida de confidencialidad, uso inapropiado o perdida de integridad).
8	**OPERACIÓN**		

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.1 3.6	Principios y lineamientos Metodología de Continuidad del Negocio	No aplica	En los apartes del manual Sistema de Gestión de continuidad del negocio, se mencionan los responsables y las actividades que deben realizar, propendiendo en ellos la documentación adecuada que debe de existir de los procesos y los planes de continuidad generados para estos.	No aplica	
3.1 3.6	Principios y lineamientos Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad		No aplica	
	No se evidencia en el documento	No aplica		En el documento no se especifican los formatos de creación y actualización, medios de comunicación de los documentos, revisión y aprobación de la información documentada, lo cual llevaría a informalidad en los procesos y las líneas de comunicación.	
3.1 3.6	Principios y lineamientos Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad		No aplica	
	No se evidencia en el documento	No aplica	No aplica	En el plan se hace énfasis en la documentación de cada proceso y plan, pero no se indica la protección de la confidencialidad, perdida de integridad, o el uso inapropiado, lo cual puede llevar a divulgación de información confidencial o controlada, perdida o adulteración de esta.	

Aparte	Sección	Descripción	
8.1	Planificación y control.	La organización debe planear, implementar y *controlar los procesos* para cumplir los requisitos para ejecutar las acciones determinadas en el numeral 6.1	Establecer los criterios para esos procesos
			Aplicar el control de estos procesos de acuerdo con los criterios
			Mantener información documentada para demostrar que los procesos se han llevado a cabo como estaba Previsto
8.2	Análisis de impacto al negocio y valoración del riesgo.		
8.2.1	Generalidades	La organización debe planear, implementar y mantener un proceso formal y documentado para el análisis de impacto al negocio y valoración del riesgo	Establece el marco de la valoración, define los criterios y evalúa el impacto potencial de un incidente perjudicial.
			Toma en cuenta los requisitos legales y otros que la organización suscriba.
			Incluye un análisis sistemático, la priorización de los tratamientos de riesgo y sus costos relacionados.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.2 Desarrollar e implementar la continuidad de negocio 3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	**90,32%**
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.2 Desarrollar e implementar la continuidad de negocio 3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	No aplica	En el análisis de impacto al negocio (BIA), se hace referencia al análisis sistemático y a la priorización de los tratamientos de riesgo pero no se hace referencia a los costos relacionados o donde revisarlos, lo que conlleva a desconocer financieramente el costo del impacto.	

Aparte	Sección	Descripción	
			Define la salida necesaria del análisis de impacto al negocio y valoración del riesgo.
			Especifica los requisitos para que esta información se mantenga actualizada y confidencial.
8.2.2	Análisis del impacto del negocio	La organización debe establecer, implementar y mantener un proceso de evaluación formal y documentado para determinar las prioridades de continuidad y recuperación, objetivos y metas .	La identificación de actividades que apoyan la prestación de bienes y servicios.
			La evaluación de los impactos en el tiempo de no realizar estas actividades.
			El establecimiento de plazos prioritarios para la reanudación de estas actividades a un nivel mínimo especificado aceptable, teniendo en cuenta los impactos de la no reanudación de ellas será inaceptable.
			La identificación de dependencias y recursos de apoyo para estas actividades, incluyendo proveedores, subcontratados, socios y otras partes interesadas pertinentes.
8.2.3	Valoración del riesgo	La organización debe establecer, implementar y mantener un proceso formal de valoración del riesgo documentado que sistemáticamente identifica analiza y evalúa el riesgo de	Identificar los riesgos de la interrupción de las actividades prioritarias de la organización y los procesos, sistemas de información, persona, bienes, proveedores y otros recursos que los apoyan.
			Analizar sistemáticamente el riesgo.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio	No aplica	En el documento se describen los requisitos para actualizar la información pero no se hace referencia al tipo de tratamiento de confidencialidad frente a la misma, lo que puede acarrear que la información sensible sea de conocimiento público.	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA 3.6.4 Evaluación de proveedores críticos	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.4 Evaluación de proveedores críticos	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.4 Evaluación de proveedores críticos	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de	No aplica	No aplica	

Aparte	Sección	Descripción	
		incidentes perjudiciales a la organización.	
			Evaluar los riesgos relacionados con la interrupción que requieren tratamiento.
			Identificar tratamientos acordes con los objetivos de continuidad de negocio y de acuerdo con el apetito de riesgo de la organización.
8.3	Estrategia de continuidad de negocio.		
8.3.1.	Determinación y selección	Basarse en los resultados de los análisis de impacto al negocio y valoración del riesgo. (La determinación de la estrategia debe incluir la aprobación de marcos de prioridad de tiempo para la reanudación de las actividades).	Proteger las actividades prioritarias.
			Estabilizar, continuar, reanudar y recuperar las actividades priorizadas y sus dependencias y recursos de apoyo.
			Mitigar, responder y gestionar impactos
8.3.2	Establecimiento de las necesidades de recursos	La organización debe determinar las necesidades de recursos para poner en práctica las estrategias	Las persona

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
		impacto al negocio – BIA			
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad	No aplica	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el documento acerca de la identificación y documentación del apetito de riesgo del Banco por lo cual no están identificados los posibles tratamientos acordes con los objetivos de continuidad del negocio, esto conlleva a medidas no adecuadas de cuantificación de impacto sobre los objetivos de negocio.	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	Subtitulo - Identificación de procesos críticos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta 3.6.6 Definición de planes de respuesta y manejo de crisis	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta	No aplica	No aplica	
3.3 3.6	Recursos y presupuesto. Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA	Recursos críticos	No aplica	

Aparte	Sección	Descripción	
		seleccionadas. Los tipos de recursos considerados se incluyen, pero no se limitan a:	La información y los datos
			Los edificios, el ambiente de trabajo y servicios asociados.
			Instalaciones, equipos y consumibles
			El sistema de información y la tecnología de comunicación
			El transporte
			La financiación
			Socios y proveedores.
8.3.3	Protección y mitigación.	Para los riesgos identificados que requieren tratamiento la organización debe considerar medidas proactivas que:	Reduzcan la probabilidad de interrupción
			Acorten el período de interrupción

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.3 3.6	Recursos y presupuesto Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	Recursos críticos	No aplica	
3.3 3.6	Recursos y presupuesto Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad	No aplica	No aplica	
3.3 3.6	Recursos y presupuesto Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA 3.6.5 Definición y diseño de estrategias de respuesta	Recursos críticos Estrategias de recuperación	No aplica	
3.3 3.6	Recursos y presupuesto Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	Recursos críticos	No aplica	
3.2	Gobierno de Continuidad de negocio	3.2.1 Roles y responsabilidades	Equipos de logística	No aplica	
3.3	Recursos y presupuesto			No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.4 Evaluación de proveedores críticos.	Junta Directiva	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.5 Definición y diseño de estrategias de respuesta	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA 3.6.5 Definición y diseño de estrategias de respuesta	No aplica		

Aparte	Sección	Descripción	
			Limiten el impacto de la interrupción de los productos clave de la organización y servicios
8.4	Establecer e implementar procedimientos de continuidad de negocio.		
8.4.1	Generalidades	Establecer e implementar procedimientos de continuidad de negocio.	Establecer un protocolo de comunicaciones interno y externo adecuado
			Ser específicos con respecto a las medidas inmediatas que deben tomarse durante una interrupción
			Ser flexibles para responder a amenazas imprevistas y las cambiantes condiciones internas y externas
			Centrarse en el impacto de los eventos que podrían potencialmente interrumpir las operaciones
			Ser desarrollados en base a los supuestos establecidos y el análisis de las interdependencias.
			Ser eficaces en la reducción de sus consecuencias a través de la aplicación de estrategias apropiadas de mitigación.
8.4.2	Estructura de respuesta ante incidentes	La estructura de la respuesta debe:	Identificar los umbrales de los efectos que justifiquen la iniciación de la respuesta formal.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.5 Definición y diseño de estrategias de respuesta	No aplica		
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	Plan comunicación de crisis	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	Plan de recuperación de procesos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.2 Evaluación de riesgos de continuidad 3.6.3 Análisis de impacto al negocio – BIA		No aplica	
3.1 3.6	Principios y lineamientos Metodología de Continuidad del Negocio	3.6.3 Análisis de impacto al negocio – BIA	- Actividades permanentes del SGCN / Criterios en la selección de estrategias. - Impacto Cualitativo _ Impacto Cuantitativo	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta	Criterio selección de estrategias, estrategias de mitigación.	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta	Criterio selección de estrategias, estrategias de mitigación.	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	Plan de administración de crisis	No aplica	

Aparte	Sección	Descripción	
			Evaluar la naturaleza y el alcance de un incidente perjudicial y su impacto potencial.
			Activar una respuesta apropiada de Continuidad de negocio.
			Tener procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta.
			Tener los recursos disponibles para apoyar los procesos y procedimientos para manejar un incidente perjudicial para minimizar el impacto.
			Comunicarse con las partes interesadas y las autoridades, así como los medios de comunicación.
8.4.3	Advertencia y comunicación.	La organización debe establecer, implementar y mantener procedimientos:	La detección de un incidente.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	No se evidencia en el documento	No aplica	No aplica	En la estructura de la respuesta no se hace referencia a la evaluación de la naturaleza, del alcance y del impacto potencial del incidente, lo cual puede conllevar a la subvaloración del incidente por parte de los interesados.	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	- Plan de recuperación de procesos - Planes o procedimientos de Contingencia de procesos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	- Plan de comunicación de crisis - Planes o procedimientos de Contingencia de procesos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	- Plan de recuperación de procesos - Planes o procedimientos de Contingencia de procesos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición de planes de respuesta y manejo de crisis	Plan de administración de crisis	No aplica	
3.2 3.4	Gobierno de Continuidad de negocio Proceso de Gestión de continuidad de negocio	3.2.1 Roles y responsabilidades 3.4.2 Desarrollar e implementar la continuidad de negocio	- Director de tecnología informática y calidad de TI – Líder de recuperación ante desastres, Líder de recuperación de procesos	No aplica	

Aparte	Sección	Descripción	
			El seguimiento regular de un incidente.
			La comunicación interna dentro de la organización y recibir, documentar y responder a la comunicación de las partes interesadas.
			Recibir, documentar y responder a cualquier sistema de alerta de riesgo a nivel nacional o regional o su equivalente.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.6 Definición de planes de respuesta y manejo de crisis	- Director de tecnología informática y calidad de TI – Líder de recuperación ante desastres, Líder de recuperación de procesos, Líder de plan de manejo de emergencias - Plan de administración de crisis	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.6 Definición de planes de respuesta y manejo de crisis	- Director de tecnología informática y calidad de TI – Líder de recuperación ante desastres, Gerente de comunicaciones e investigación - Líder del plan de comunicación de crisis, Equipo de comunicación de crisis. - Plan de comunicación de crisis	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.10 Mantener estrategias, planes y documentación de continuidad	Líder de gestión de continuidad de negocio, Director de tecnología informática y calidad de TI – Líder de recuperación ante desastres, Líder de gestión de continuidad de tecnología.	No aplica	

Aparte	Sección	Descripción	
			Asegurar la disponibilidad de los medios de comunicación durante un incidente perjudicial.
			Facilitar la comunicación estructurada con los servicios de emergencia.
			Registrar la información vital sobre el incidente, las medidas adoptadas y las decisiones tomadas, y lo siguiente será considerado e implementado, donde aplique.
8.4.4	Planes de continuidad de negocio	La organización debe tener procedimientos documentados para restaurar y retomar las actividades de negocio, de las medidas temporales adoptadas para soportar las necesidades normales del negocio después de un incidente.	
		Los planes de continuidad deben tener colectivamente:	Un proceso para la activación de la respuesta
			Los detalles para gestionar las consecuencias inmediatas de un incidente perjudicial teniendo en cuenta: - El bienestar de los individuos. - Las opciones estratégicas, tácticas y operativas para la respuesta a la interrupción. - La prevención de la pérdida o no disponibilidad de las actividades prioritarias.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.6 Definición de planes de respuesta y manejo de crisis	Gerente de comunicaciones e investigación (líder del plan de comunicación de crisis) - Equipo de comunicación de crisis. Plan comunicación de crisis	No aplica	
3.2 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.6 Definición de planes de respuesta y manejo de crisis	Gerente de comunicaciones e investigación (líder del plan de comunicación de crisis) - Equipo de comunicación de crisis. Plan comunicación de crisis	No aplica	
3.2 3.4	Gobierno de Continuidad del Negocio Proceso de Gestión de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.4.3 Verificar y revisar la continuidad de negocio	Comité de manejo de crisis	No aplica	
3.2. 3.6	Gobierno de Continuidad del Negocio Metodología de Continuidad del Negocio	3.2.1 Roles y responsabilidades 3.6.6 Definición de planes de respuesta y manejo de crisis	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	Plan comunicación de crisis	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	- Plan de administración de crisis - Planes de prevención, preparación y respuesta ante emergencias	No aplica	

Aparte	Sección	Descripción	
			La información detallada sobre cómo y bajo qué circunstancias la organización se comunicará con los empleados y sus familiares las partes interesadas claves y los contactos de emergencia.
			Cómo la organización va a continuar o recuperar sus actividades prioritarias dentro de los plazos predeterminados.
			Los detalles de la respuesta de la organización de los medios de comunicación a raíz de un incidente, incluyendo: - Estrategia de comunicación. - La interfaz seleccionada con los medios de comunicación. - Guía o plantilla para la redacción de una declaración para los medios de comunicación. -Portavoces apropiados.
			Un proceso para levantarse una vez que el incidente ha terminado. EL PLAN DEBE DEFINIR: - Propósito y alcance - Objetivos - Criterios y procedimientos de activación - Procedimientos de implementación - Roles responsabilidades y autoridades - Requisitos y procedimientos de comunicación - Interdependencias internas y externas y las interacciones - Necesidades de recursos y - Flujo de información y procesos de documentación
8.4.5	Recuperación	La organización debe tener procedimientos documentados para restaurar y retornar las actividades de negocio, de las medidas temporales adaptadas para soportar las necesidades normales del negocio después de un incidente.	

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	Plan comunicación de crisis	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta 3.6.6 Definición planes de respuesta y manejo de crisis.	Plan de Contingencia y recuperación de Tecnología – DRP y Plan de recuperación de procesos	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.6 Definición planes de respuesta y manejo de crisis.	Plan comunicación de crisis	En el documento no hay referencia en la respuesta de la organización en un incidente en cuanto a la estrategia, la interfaz y la guía o plantilla para la declaración a los medios de comunicación, lo cual puede provocar fallos en los controles de la información divulgada.	
	No se evidencia en el documento	No aplica	No aplica	No se evidencia en el documento referencia al proceso a seguir para levantar el BCP una vez haya finalizado el incidente en la organización, lo cual puede provocar desarticulación de los procesos a realizar.	
3.6	Metodología de Continuidad del Negocio	3.6.5 Definición y diseño de estrategias de respuesta 3.6.6 Definición planes de respuesta y manejo de crisis.	- Criterios en la selección de Estrategias / Estrategias de recuperación - Plan de Contingencia y recuperación de	No aplica	

Aparte	Sección	Descripción	
8.5	Ejercicios y pruebas	La organización debe hacer ejercitar y probar sus procedimientos de continuidad de negocio para asegurar que sean compatibles con sus objetivos de continuidad de Negocio.	Sean consistentes con el alcance y los objetivos del BCMS.
			Se basen en escenarios apropiados que están bien planificados, con objetivos claramente definidos
			Tomen en conjunto con el tiempo validado la totalidad de los acuerdos de continuidad de negocio, involucrando las partes interesadas pertinentes
			Reduzcan al mínimo el riesgo de interrupción de las operaciones.
			Produzcan formalmente, después del ejercicio, informes que contengan los resultados, recomendaciones y acciones a implementar.
			Revisen en el contexto de la promoción de la mejora continua.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
			Tecnología – DRP - Plan de recuperación de procesos críticos		
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	El aparte de la realización de las pruebas especifica el diseño, la ejecución, evaluación y las oportunidades de mejora que brindan. Y adicionalmente en todo el documento existe la premisa de realizarlas y mantenerlas, y los roles que deben tener a cargo estas pruebas.	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes		No aplica	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.9 Realizar pruebas a estrategias y planes		No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes		No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes		No aplica	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.9 Realizar pruebas a estrategias y planes		No aplica	

Aparte	Sección	Descripción	
			Se lleven a cabo a intervalos planificados, y cuando hay cambios significativos dentro de la organización o el medio ambiente en el que opera
9	**EVALUACIÓN DE DESEMPEÑO**		
9.1	Seguimientos, Medición, Análisis y evaluación.		
9.1.1	Generalidades	La organización debe determinar:	Que necesita ser monitoreado y medido.
			Los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar la validez de los resultados
			Cuándo el seguimiento y la medición se llevarán a cabo.
			Cuándo los resultados del seguimiento y medición deben ser analizados y evaluados.
		La organización debe mantener información documentada como evidencia de los resultados.	

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes		No aplica	
					65,38%
	No se evidencia en el documento	No aplica	No aplica	En el plan se habla del monitoreo como responsabilidades de los comités al momento de presentarse un evento, pero no hace referencia al seguimiento de los procesos con el ánimo de establecer que debe ser monitoreado con el fin de ser sometidos a pruebas.	
3.5 3.6	Métricas y medición de la gestión de continuidad del negocio Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	

Aparte	Sección	Descripción	
		La organización debe evaluar el desempeño del BCMS y su eficacia.	
		Además, la organización debe: - Tomar acciones cuando sea necesario para hacer frente a las tendencias adversas o resultados antes de una no conformidad, y - conservar la información documentada pertinente como evidencia los resultados. Los procedimientos para seguimiento del desempeño deben proveer: - El establecimiento de indicadores de desempeño adecuados a las necesidades de la organización, - El seguimiento de la medida en que se cumplan las políticas de Continuidad de Negocio de la organización, los objetivos y metas. - El desempeño de los procesos, procedimientos y funciones que protegen sus actividades prioritarias - El control del cumplimiento con esta norma y los objetivos de continuidad de negocio, - El seguimiento de la evidencia histórica de los resultados deficientes del desempeño del BCMS. - El registro de datos y los resultados de seguimiento y medición para facilitar las acciones correctivas tomadas.	
9.1.2	Evaluación de los procedimientos de continuidad de negocio		La organización debe llevar a cabo evaluaciones de sus procedimientos de Continuidad de Negocio y capacidades para asegurar su continua adecuación, idoneidad y eficacia.
			Las evaluaciones deben llevarse a cabo a través de revisiones periódicas, ejercicios, pruebas, reportes después de incidentes y evaluaciones de desempeño, los cambios significativos que surgen deben ser reflejados en el procedimiento de manera oportuna.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	Continuidad del Negocio				
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.1 3.4 3.5 3.6	Principios y Lineamientos Proceso de Gestión de Continuidad del Negocio Métricas y medición de la gestión de continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.5.1 Medición de la cultura de continuidad 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	

Aparte	Sección	Descripción	
			Se debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentarios, mejores prácticas industriales, y la conformidad con su propia política y objetivos de continuidad de negocio.
			La organización debe llevar a cabo evaluaciones e intervalos planificados cuando se produzcan cambios significativos.
9.2	Auditoria interna	La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el BCMS	Se ajusta a: - Los requisitos propios de la organización para su BCMS - Los requisitos de esta norma.
			Es eficazmente implementado y mantenido

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	No se evidencia en el documento	No aplica	No aplica	En el documento no se hace referencia a la evaluación de la metodología utilizada frente a nuevos métodos, mejores prácticas, o nuevas normativas, lo cual puede provocar desactualización del BCP en cuanto requisitos legales y mejores prácticas de operación.	
3.4 3.6	Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio a) Realizar auditoría al SGCN	No aplica	El documento no está ajustado totalmente a todos los requisitos solicitados en la norma NTC 5722	
3.1 3.4 3.6	Principios y Lineamientos Proceso de Gestión de Continuidad del Negocio Metodología de Continuidad del Negocio	3.4.2 Desarrollar e implementar la continuidad de negocio 3.4.4 Actuar, mantener y mejorar la continuidad del negocio	No aplica	No aplica	

Aparte	Sección	Descripción	
			La organización debe: - Planear establecer implementar y mantener un programa de auditoría incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y resultados. Los programas de auditoría deben tener en consideración la importancia de los procesos y de los resultados de auditorías anteriores.
			Definir los criterios de auditoría y el alcance de cada una
			Seleccionar auditores y gestionar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría.
			Garantizar que los resultados de auditoría son reportados a la dirección.
			Mantener información documentada como evidencia de la implementación del programa de auditoría y de sus resultados.
9.3	Revisión por la dirección	La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para asegurar su continua idoneidad, adecuación y	El estado de las acciones de las revisiones por la dirección previas.
			Los cambios en los asuntos internos y externos que son pertinentes para el BCMS.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio a) Realizar auditoría al SGCN	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio a) Realizar auditoría al SGCN	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio a) Realizar auditoría al SGCN	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio b) Revisar el SGCN por parte de la alta dirección	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio Tabla 3 Tareas de verificación y revisión Continuidad de Negocio	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio b) Revisar el SGCN por parte de la alta dirección	No aplica	No aplica	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio b) Revisar el SGCN por parte de la alta dirección	No aplica	No aplica	

Aparte	Sección	Descripción	
		eficacia. (La revisión por la dirección debe incluir la consideración de):	Información sobre el desempeño de Continuidad de Negocio, incluyendo las tendencias en: - Las no conformidades y acciones correctivas. - El seguimiento y la evaluación de resultados de la medición. - Resultado de la auditoría.
			Las oportunidades de mejora continua.
			Las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique. -Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas. - Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	No se evidencia en el documento	No aplica	No aplica	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN .	
3.4	Proceso de gestión continuidad del negocio	3.4.3 Verificar y revisar la continuidad de negocio b) Revisar el SGCN por parte de la alta dirección	No aplica	No aplica	
	No se evidencia en el documento	No aplica	No aplica	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluyen que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en: - La necesidad de cambios en el BCMS, incluyendo la política y los objetivos. - Los resultados de las auditorías y revisiones al BCMS, incluidos los de los principales proveedores y socios, cuando aplique. -Las técnicas, productos o procedimientos, que podrían ser utilizados en la organización	

Aparte	Sección	Descripción	
			Variaciones en el alcance del BCMS

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
				para mejorar el desempeño y eficacia del BCMS. - El estado de acciones correctivas. - Los resultados de los ejercicios y pruebas. - Los riesgos o problemas no abordados adecuadamente en cualquier valoración del riesgo anterior. - Cualquier cambio que pudiera afectar el BCMS, ya sea interna o externa al alcance del BCMS. - La adecuación de la política. - Las lecciones aprendidas y las acciones derivadas de incidentes perjudiciales. - Buenas prácticas y guías emergentes. Generando una posible falta de gestión de las partes interesadas respecto a los ajustes propios de los BCMS, considerados por la revisiones efectuada de las altas directivas,	
	No se evidencia en el documento	No aplica	No aplica	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluye que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en las variaciones en el alcance del BCMS, Que puede conllevar a acciones ineficaces para el control de un evento, puesto que se están dejando por fuera posibles procesos por las variaciones del negocio.	

Aparte	Sección	Descripción	
			Mejoramiento de la eficacia del BCMS
			Actualización de la valoración del riesgo, BIA, planes de continuidad de negocio, y procedimientos relacionados.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
	No se evidencia en el documento	No aplica	No aplica	Dentro del manual no se especifican las acciones nombradas en el aparte de la norma, se indica escuetamente en numeral 3.4 y 3.5 acciones de la alta dirigencia en cuanto a la revisión del SGCN cuando existan cambios significativos, y en los roles y responsabilidades de las altas directivas pronunciarse sobre la evaluación del SGCN. Pero no se incluyen que en las revisiones efectuadas por la alta dirección se debe considerar el desempeño de la organización en el mejoramiento de la eficacia del BCMS, lo que conlleva a la ausencia de una búsqueda del mejoramiento continuo, y una contrariedad al énfasis dado por el mismo manual en el mejoramiento y mantenimiento de las estrategias de continuidad de negocio.	
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	

Aparte	Sección	Descripción	
			Modificación de los procedimientos y controles para responder a los eventos internos o externos que pueden afectar al BCMS, incluidos los cambios; - Los requisitos del negocio y operacionales. - Reducción de riesgos y requisitos de seguridad. - Condiciones y procesos de operación. - Requisitos legales y reglamentarios. - Obligaciones contractuales. - Los niveles de riesgo y/o criterios de aceptación de riesgos. - Recursos necesarios. - La financiación y las necesidades presupuestarias.
			Como la eficacia de los controles son medidas.
		La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección. La organización debe:	- Comunicar los resultados de examen de la gestión de las partes interesadas y pertinentes. - Tomar las medidas apropiadas en relación con esos resultados.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.6	Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el manual sobre la medición de la eficacia de los controles por parte de la alta dirección, lo cual puede provocar el desconocimiento del nivel en el cual las actividades planeadas son realizadas y los resultados planeados son alcanzados.	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el manual a la documentación generada por la alta dirección frente a la revisión realizada y a las medidas tomadas con base a los resultados, lo cual puede provocar incoherencias entre las medidas tomadas por la alta dirección y los intereses de las partes.	

Aparte	Sección	Descripción	
10	**MEJORA**		
10.1	No conformidad y acción correctiva	Cuando ocurra una no conformidad, la organización debe:	Identificar la no conformidad.
			Responder a las no conformidades, y, cuando aplique: - Tomar medidas para controlarlas y corregirlas. - Tratar con las consecuencias.
			Evaluar la necesidad de adoptar medidas para eliminar las causas de la no conformidad, para que así no se repita o se produzca en otra parte, incluyendo: - La revisión de las no conformidades. - La determinación de las causas de no conformidades. - La determinación de no conformidades similares existentes, o que potencialmente pudieran ocurrir. - La evaluación de la necesidad de acciones correctivas para asegurar que las no conformidades no se repitan o se produzcan en otros lugares. - La determinación e implementación de las acciones correctivas necesarias. - La revisión de la eficacia de cualquier acción correctiva tomada. - La elaboración de cambios al BCMS, si es necesario.

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.6.9 Realizar pruebas a estrategias y planes	Seguimiento a hallazgos y oportunidades de mejora	No aplica	**86%**
3.6 3.4	Metodología de Continuidad del Negocio Proceso de gestión continuidad del negocio	3.6.9 Realizar pruebas a estrategias y planes 3.6.10 Mantener estrategias, planes y documentación de continuidad 3.4.4 Actuar, mantener y mejorar la continuidad del negocio	Seguimiento a hallazgos y oportunidades de mejora	No aplica	
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.3 Verificar y revisar la continuidad de negocio 3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	

Aparte	Sección	Descripción	
			Implementar cualquier acción requerida.
			Revisar la eficacia de cualquier acción tomada.
			Hacer los cambios al BCMS, si es necesario.
10.2	Mejora continua	La organización debe mejorar continuamente la idoneidad, adecuación o eficacia del BCMS.	

Aparte	Sección	Subsección	Aclaraciones	Hallazgo	%
3.4 3.6	Proceso de gestión continuidad del negocio Metodología de Continuidad del Negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio 3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	
	No se evidencia en el documento	No aplica	No aplica	No se hace referencia en el manual sobre la medición de la eficacia de cualquier acción tomada frente a una no conformidad, lo cual puede provocar el desconocimiento del nivel en el cual las actividades planeadas son realizadas y los resultados planeados son alcanzados.	
3.4	Proceso de gestión continuidad del negocio	3.4.4 Actuar, mantener y mejorar la continuidad del negocio	No aplica	No aplica	
3.6	Metodología de Continuidad del Negocio	3.6.10 Mantener estrategias, planes y documentación de continuidad	No aplica	No aplica	

Fuente: Elaboración de los autores, adaptada de la Norma Técnica Colombiana NTC 5722 Sistemas de gestión de continuidad de Negocio Requisitos y el manual del Sistema de Gestión de Continuidad del Negocio de la entidad bancaria.